

J.W. Ence  
949/261,8433  
makoto Tatebayashi et al.

日 本 国 特 許 庁  
PATENT OFFICE NAKI-BI69  
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されて  
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed  
with this Office.

出 願 年 月 日  
Date of Application:

1998年11月30日

出 願 番 号  
Application Number:

平成10年特許願第339027号

出 願 人  
Applicant(s):

松下電器産業株式会社

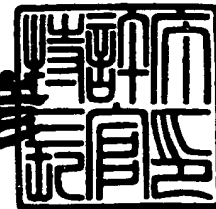


CERTIFIED COPY OF  
PRIORITY DOCUMENT

1999年10月 1日

特許庁長官  
Commissioner,  
Patent Office

近 藤 隆 彦



出証番号 出証特平11-3066903

【書類名】 特許願

【整理番号】 2022500492

【提出日】 平成10年11月30日

【あて先】 特許庁長官 殿

【国際特許分類】 G09C 1/00

【発明の名称】 デジタル著作物保護システム

【請求項の数】 24

【発明者】

（ 【住所又は居所】 大阪府門真市大字門真 1006 番地 松下電器産業株式会社内

【氏名】 原田 俊治

【発明者】

【住所又は居所】 大阪府門真市大字門真 1006 番地 松下電器産業株式会社内

【氏名】 館林 誠

【発明者】

【住所又は居所】 大阪府門真市大字門真 1006 番地 松下電器産業株式会社内

【氏名】 小塚 雅之

【発明者】

【住所又は居所】 大阪府門真市大字門真 1006 番地 松下電器産業株式会社内

【氏名】 中村 穰

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100090446

【弁理士】

【氏名又は名称】 中島 司朗

【代理人】

【識別番号】 100109210

【弁理士】

【氏名又は名称】 新居 広守

【先の出願に基づく優先権主張】

【出願番号】 平成10年特許願第295920号

【出願日】 平成10年10月16日

【手数料の表示】

【予納台帳番号】 014823

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9810105

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 デジタル著作物保護システム

【特許請求の範囲】

【請求項 1】 記録媒体とアクセス装置とが接続された状態で、両者間で機器認証フェーズと著作物転送フェーズとを実行して著作物の正当者への配布を実現するデジタル著作物保護システムであって、

機器認証フェーズでは、記録媒体が所有する固有鍵をアクセス装置に秘密伝送し、アクセス装置が取得した固有鍵を用いて、機器認証を行い、

著作物転送フェーズでは、機器認証が成功した場合にのみ、アクセス装置が取得した固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する

ことを特徴とするデジタル著作物保護システム。

【請求項 2】 記録媒体とアクセス装置とが接続された状態で、前記記録媒体と前記アクセス装置との間で機器認証と暗号化された著作物の転送とを行うデジタル著作物保護システムであって、

前記記録媒体は、

記録媒体毎に異なる固有鍵を予め記憶している固有鍵記憶領域と、

接続されたアクセス装置へ前記固有鍵を秘密伝送し、前記固有鍵を用いて前記アクセス装置との間で機器認証を行う第 1 認証手段と、

前記固有鍵を用いて暗号化される著作物を保持するための領域とを備え、

前記アクセス装置は、

記録媒体から秘密伝送された固有鍵を用いて、前記記録媒体との間で機器認証を行う第 2 認証手段と、

機器認証が成功した場合にのみ、前記機器認証を経て得た固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する転送手段とを備える

ことを特徴とするデジタル著作物保護システム。

【請求項 3】 前記第 1 認証手段は、あらかじめ第 1 鍵を有し、前記第 1 鍵を用いて、前記固有鍵に第 1 暗号を施して暗号化固有鍵を生成して伝送し、

前記第 2 認証手段は、あらかじめ前記第 1 鍵を有し、前記第 1 鍵を用いて、前記伝送された暗号化固有鍵に、前記第 1 暗号の逆変換を行う第 1 復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、

前記転送手段は、前記復号固有鍵を用いて著作物の転送を行う

ことを特徴とする請求項 2 記載のデジタル著作物保護システム。

【請求項 4】 前記第 1 認証手段は、第 1 鍵を基にして、公開鍵暗号方式の公開鍵決定アルゴリズムにより算出された公開鍵である第 2 鍵をあらかじめ有し、前記第 2 鍵を用いて、前記固有鍵に第 1 暗号を施して暗号化固有鍵を生成して伝送し、

前記第 2 認証手段は、あらかじめ前記第 1 鍵を有し、前記第 1 鍵を用いて、前記伝送された暗号化固有鍵に、前記第 1 暗号の逆変換を行う第 1 復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、

前記転送手段は、前記復号固有鍵を用いて著作物の転送を行う

ことを特徴とする請求項 2 記載のデジタル著作物保護システム。

【請求項 5】 前記第 1 認証手段は、あらかじめ第 1 鍵を有し、前記第 1 鍵を用いて、前記固有鍵に回復型署名処理を施して署名文を生成して伝送し、

前記第 2 認証手段は、前記第 1 鍵に前記回復型署名処理の公開鍵決定アルゴリズムにより算出された公開鍵である第 2 鍵をあらかじめ有し、前記第 2 鍵を用いて、前記伝送された署名文に、前記回復型署名の検証処理を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、

前記転送手段は、前記復号固有鍵を用いて著作物の転送を行う

ことを特徴とする請求項 2 記載のデジタル著作物保護システム。

【請求項 6】 前記デジタル著作物保護システムは、さらに

固有鍵に第 1 暗号を施して暗号化固有鍵に変換する固有鍵変換手段を備える暗号化固有鍵作成装置を有し、

前記第 1 認証手段は、前記固有鍵を前記固有鍵変換手段へ出力して変換された暗号化固有鍵を受け取り、受け取った暗号化固有鍵を前記アクセス装置へ伝送し

前記第 2 認証手段は、記録媒体から伝送された暗号化固有鍵に前記第 1 暗号の逆処理を行う第 1 復号を施して固有鍵を生成する

ことを特徴とする請求項 2 記載のデジタル著作物保護システム。

【請求項 7】 前記第 1 認証手段は、あらかじめ複数の第 1 鍵を有し、前記複数の第 1 鍵のうち一つの第 2 鍵の選択を受け付け、前記第 2 鍵を用いて、前記固有鍵に第 1 暗号を施して暗号化固有鍵を生成して伝送し、

前記第 2 認証手段は、あらかじめ複数の第 1 鍵を有し、前記複数の第 1 鍵から前記第 2 鍵の選択を受け付け、前記第 2 鍵を用いて、前記伝送された暗号化固有鍵に、前記第 1 暗号の逆変換を行う第 1 復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、

前記転送手段は、前記復号固有鍵を用いて著作物の転送を行う

ことを特徴とする請求項 2 記載のデジタル著作物保護システム。

【請求項 8】 アクセス装置と接続された状態で、前記アクセス装置との間で機器認証と暗号化された著作物の転送とを行う記録媒体であって、

記録媒体毎に異なる固有鍵を記憶している固有鍵記憶領域と、

前記固有鍵を用いて暗号化される著作物を保持するための領域と、

アクセス装置が接続されたとき、記録媒体から当該アクセス装置へ固有鍵を秘密伝送する手順を経て、当該アクセス装置との間で機器認証を行う認証手段と、

機器認証が成功した場合にのみ、前記固有鍵を用いて暗号化された著作物を受け取り前記領域に書き込み若しくは前記領域に記憶されている暗号化された著作物を読み出して前記アクセス装置へ出力する転送手段と

を備えることを特徴とする記録媒体。

【請求項 9】 固有鍵を有する記録媒体と接続され、前記記録媒体との間で機器認証と暗号化された著作物の転送とを行うアクセス装置であって、

記録媒体から固有鍵を秘密伝送される手順を経て、前記記録媒体との間で機器認証を行う認証手段と、

機器認証が成功した場合にのみ、前記機器認証を経て得た固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号

する転送手段と

を備えることを特徴とするアクセス装置。

【請求項 10】 記録媒体とアクセス装置とが接続された状態で、両者間で機器認証ステップと著作物転送ステップとを実行して著作物の正当者への配布を実現するデジタル著作物保護方法であって、

機器認証ステップでは、記録媒体が所有する固有鍵をアクセス装置に秘密伝送し、アクセス装置が取得した固有鍵を用いて、機器認証を行い、

著作物転送ステップでは、機器認証が成功した場合にのみ、アクセス装置が取得した固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する

ことを特徴とするデジタル著作物保護方法。

【請求項 11】 記録媒体毎に異なる固有鍵を予め記憶している固有鍵記憶領域及び前記固有鍵を用いて暗号化される著作物を保持するための領域を有する記録媒体とアクセス装置とが接続された状態で、前記記録媒体と前記アクセス装置との間で機器認証と暗号化された著作物の転送とを行うデジタル著作物保護システムで用いられるデジタル著作物保護方法であって、

接続されたアクセス装置へ前記固有鍵を秘密伝送し、前記固有鍵を用いて前記アクセス装置との間で機器認証を行う第 1 認証ステップと、

記録媒体から秘密伝送された固有鍵を用いて、前記記録媒体との間で機器認証を行う第 2 認証ステップと、

機器認証が成功した場合にのみ、前記機器認証を経て得た固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する転送ステップとを

含むことを特徴とするデジタル著作物保護方法。

【請求項 12】 前記第 1 認証ステップは、あらかじめ第 1 鍵を有し、前記第 1 鍵を用いて、前記固有鍵に第 1 暗号を施して暗号化固有鍵を生成して伝送し、前記第 2 認証ステップは、あらかじめ前記第 1 鍵を有し、前記第 1 鍵を用いて、前記伝送された暗号化固有鍵に、前記第 1 暗号の逆変換を行う第 1 復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認

証を行い、

前記転送ステップは、前記復号固有鍵を用いて著作物の転送を行う

ことを特徴とする請求項 11 記載のデジタル著作物保護方法。

【請求項 13】 前記第 1 認証ステップは、第 1 鍵を基にして、公開鍵暗号方式の公開鍵決定アルゴリズムにより算出された公開鍵である第 2 鍵をあらかじめ有し、前記第 2 鍵を用いて、前記固有鍵に第 1 暗号を施して暗号化固有鍵を生成して伝送し、

前記第 2 認証ステップは、あらかじめ前記第 1 鍵を有し、前記第 1 鍵を用いて、前記伝送された暗号化固有鍵に、前記第 1 暗号の逆変換を行う第 1 復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、

前記転送ステップは、前記復号固有鍵を用いて著作物の転送を行う

ことを特徴とする請求項 11 記載のデジタル著作物保護方法。

【請求項 14】 前記第 1 認証ステップは、あらかじめ第 1 鍵を有し、前記第 1 鍵を用いて、前記固有鍵に回復型署名処理を施して署名文を生成して伝送し、

前記第 2 認証ステップは、前記第 1 鍵に前記回復型署名処理の公開鍵決定アルゴリズムにより算出された公開鍵である第 2 鍵をあらかじめ有し、前記第 2 鍵を用いて、前記伝送された署名文に、前記回復型署名の検証処理を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、

前記転送ステップは、前記復号固有鍵を用いて著作物の転送を行う

ことを特徴とする請求項 11 記載のデジタル著作物保護方法。

【請求項 15】 前記デジタル著作物保護システムは、さらに固有鍵に第 1 暗号を施して暗号化固有鍵に変換する固有鍵変換手段を備える暗号化固有鍵作成装置を有し、

前記第 1 認証ステップは、前記固有鍵を前記固有鍵変換手段へ出力して変換された暗号化固有鍵を受け取り、受け取った暗号化固有鍵を前記アクセス装置へ伝送し、

前記第 2 認証ステップは、記録媒体から伝送された暗号化固有鍵に前記第 1 暗号の逆処理を行う第 1 復号を施して固有鍵を生成する



ことを特徴とする請求項 11 記載のデジタル著作物保護方法。

【請求項 16】 前記第 1 認証ステップは、あらかじめ複数の第 1 鍵を有し、前記複数の第 1 鍵のうち一つの第 2 鍵の選択を受け付け、前記第 2 鍵を用いて、前記固有鍵に第 1 暗号を施して暗号化固有鍵を生成して伝送し、

前記第 2 認証ステップは、あらかじめ複数の第 1 鍵を有し、前記複数の第 1 鍵から前記第 2 鍵の選択を受け付け、前記第 2 鍵を用いて、前記伝送された暗号化固有鍵に、前記第 1 暗号の逆変換を行う第 1 復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、

前記転送ステップは、前記復号固有鍵を用いて著作物の転送を行う

ことを特徴とする請求項 11 記載のデジタル著作物保護方法。

【請求項 17】 デジタル著作物保護方法をコンピュータに実行させるためのプログラムを記録するコンピュータ読み取り可能な媒体であって、

請求項 10～16 記載の何れかのデジタル著作物保護方法をコンピュータに実行させるためのプログラムを含むことを特徴とする記録媒体。

【請求項 18】 前記第 1 認証手段は、第 3 鍵を用いて前記固有鍵に第 1 変換を施して変形鍵を生成し、

前記第 1 鍵を用いて、前記変形鍵に第 2 変換を施して、暗号化固有鍵を生成して伝送し、

前記第 2 認証手段は、前記第 1 鍵を用いて、前記伝送された暗号化固有鍵に、前記第 2 変換の逆変換を行う第 2 逆変換を施して、復号変形鍵を生成し、前記第 3 鍵を用いて、前記復号変形鍵に、前記第 1 変換の逆変換を行う第 1 逆変換を施して、復号固有鍵を生成し、前記復号固有鍵を用いて、前記記録媒体との間で機器認証を行い、

前記転送手段は、前記復号固有鍵を用いて著作物の転送を行う

ことを特徴とする請求項 2 記載のデジタル著作物保護システム。

【請求項 19】 前記第 1 認証手段は、第 1 鍵を用いて前記固有鍵に第 2 変換を施して変形鍵を生成し、前記第 3 鍵を用いて、前記変形鍵に第 1 変換を施して暗号化固有鍵を生成して伝送し、

前記第 2 認証手段は、前記第 3 鍵を用いて、前記伝送された暗号化固有鍵に、

前記第 1 変換の逆変換を行う第 1 逆変換を施して、復号変形鍵を生成し、前記第 1 鍵を用いて、前記復号変形鍵に、前記第 2 変換の逆変換を行う第 2 逆変換を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行う

ことを特徴とする請求項 2 記載のデジタル著作物保護システム。

【請求項 20】 前記第 1 認証手段は、前記第 3 鍵を用いて、第 1 鍵に第 1 変換を施して、変形第 1 鍵を生成し、前記変形第 1 鍵を用いて、前記固有鍵に第 2 変換を施して暗号化固有鍵を生成して伝送し、

前記第 2 認証手段は、前記第 3 鍵を用いて、第 1 鍵に第 1 変換を施して、変形第 1 鍵を生成し、前記変形第 1 鍵を用いて、前記伝送された暗号化固有鍵に、前記第 2 変換の逆変換を行う第 2 逆変換を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行う

ことを特徴とする請求項 2 記載のデジタル著作物保護システム。

【請求項 21】 前記第 1 認証手段は、前記第 1 鍵を用いて、前記固有鍵に第 2 変換を施して、暗号化固有鍵を生成して伝送し、前記固有鍵に第 3 鍵を用いて第 1 変換を施して変形固有鍵を生成し、

前記第 2 認証手段は、前記第 1 鍵を用いて、前記伝送された暗号化固有鍵に、前記第 1 鍵を用いて、前記第 2 変換の逆変換を行う第 2 逆変換を施して、復号固有鍵を生成し、前記復号固有鍵に第 3 鍵を用いて、第 1 変換を施して、変形復号固有鍵を生成し、前記変形復号固有鍵を用いて、前記記録媒体との間で機器認証を行い、

前記転送手段は、前記変形復号固有鍵を用いて著作物の転送を行う

ことを特徴とする請求項 2 記載のデジタル著作物保護システム。

【請求項 22】 前記著作物が、ある論理的若しくは物理的単位毎に 1 つ以上のデータブロックにより構成されているものとし、

前記著作物の各データブロックを暗号化して記録媒体に転送し、若しくは記録媒体から転送された著作物を復号する際に、

前記転送手段は、各データブロック固有のデータブロック鍵を生成し、

前記機器認証を経て得た固有鍵と、データブロック鍵とを用いて、対応するデータブロックを暗号化して、記録媒体に転送し、若しくは記録媒体から転送されたデータブロックを復号する

ことを特徴とする請求項 2 記載のデジタル著作物保護システム。

【請求項 23】 前記著作物が、1 つ以上のファイルにより構成されているものとし、

前記著作物の各ファイルを暗号化して記録媒体に転送し、若しくは記録媒体から転送された著作物を復号する際に、

前記転送手段は、各ファイル固有のファイル鍵を生成し、

前記機器認証を経て得た固有鍵と、ファイル鍵を用いて、対応するファイルを暗号化して記録媒体に転送し、若しくは記録媒体から転送されたファイルを復号する

ことを特徴とする請求項 2 記載のデジタル著作物保護システム。

【請求項 24】 前記アクセス装置は、さらに、操作者からユーザ鍵の入力を受け付けるユーザ鍵受付手段と、

前記入力を受け付けられたユーザ鍵と、記憶媒体から秘密伝送された固有鍵とを基にして、変形鍵を生成する変形鍵生成手段とを有し、

前記転送手段は、機器認証が成功した場合にのみ、前記生成された変形鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する

ことを特徴とする請求項 2 記載のデジタル著作物保護システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、デジタル化された文書、音声、画像、プログラムなどのデジタル著作物をネットワークで配信し、これを記憶媒体に記録し、携帯プレーヤで再生するシステムに関し、特に、不正にこれらの記録や再生が行われることを防ぐシステムに関する。

【0002】

【従来の技術】

近年、デジタル化された文書、音声、画像、プログラムなどのデジタル著作物がインターネットなどのネットワークを経由して流通し、利用者は、様々なデジタル著作物を簡単にネットワークを経由して取り出し、他の記録媒体に記録し、再生することができるようになってきている。

【0003】

【発明が解決しようとする課題】

しかしながら、このように簡単にデジタル著作物を複製できるという利点はあるものの、著作者の著作権が侵害されやすいという問題点がある。

本発明は、外部から取り出したデジタル著作物を不正に記録媒体へ書き込むことと、記録媒体に記録されたデジタル著作物を不正に再生することを防止するデジタル著作物保護システムを提供することを目的とする。

【0004】

【課題を解決するための手段】

上記の目的を達成するために、本発明は、記録媒体とアクセス装置とが接続された状態で、両者間で機器認証フェーズと著作物転送フェーズとを実行して著作物の正当者への配布を実現するデジタル著作物保護システムであって、機器認証フェーズでは、記録媒体が所有する固有鍵をアクセス装置に秘密伝送し、アクセス装置が取得した固有鍵を用いて、機器認証を行い、著作物転送フェーズでは、機器認証が成功した場合にのみ、アクセス装置が取得した固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号することを特徴とする。

【0005】

ここで、記録媒体とアクセス装置とが接続された状態で、前記記録媒体と前記アクセス装置との間で機器認証と暗号化された著作物の転送とを行うデジタル著作物保護システムであって、前記記録媒体は、記録媒体毎に異なる固有鍵を予め記憶している固有鍵記憶領域と、接続されたアクセス装置へ前記固有鍵を秘密伝送し、前記固有鍵を用いて前記アクセス装置との間で機器認証を行う第1認証手段と、前記固有鍵を用いて暗号化される著作物を保持するための領域とを備え、

前記アクセス装置は、記録媒体から秘密伝送された固有鍵を用いて、前記記録媒体との間で機器認証を行う第2認証手段と、機器認証が成功した場合にのみ、前記機器認証を経て得た固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する転送手段とを備えるように構成してもよい。

## 【0006】

ここで、前記第1認証手段は、あらかじめ第1鍵を有し、前記第1鍵を用いて、前記固有鍵に第1暗号を施して暗号化固有鍵を生成して伝送し、前記第2認証手段は、あらかじめ前記第1鍵を有し、前記第1鍵を用いて、前記伝送された暗号化固有鍵に、前記第1暗号の逆変換を行う第1復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

## 【0007】

ここで、前記第1認証手段は、第1鍵を基にして、公開鍵暗号方式の公開鍵決定アルゴリズムにより算出された公開鍵である第2鍵をあらかじめ有し、前記第2鍵を用いて、前記固有鍵に第1暗号を施して暗号化固有鍵を生成して伝送し、前記第2認証手段は、あらかじめ前記第1鍵を有し、前記第1鍵を用いて、前記伝送された暗号化固有鍵に、前記第1暗号の逆変換を行う第1復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

## 【0008】

ここで、前記第1認証手段は、あらかじめ第1鍵を有し、前記第1鍵を用いて、前記固有鍵に回復型署名処理を施して署名文を生成して伝送し、前記第2認証手段は、前記第1鍵に前記回復型署名処理の公開鍵決定アルゴリズムにより算出された公開鍵である第2鍵をあらかじめ有し、前記第2鍵を用いて、前記伝送された署名文に、前記回復型署名の検証処理を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

## 【0009】

ここで、前記デジタル著作物保護システムは、さらに固有鍵に第1暗号を施して暗号化固有鍵に変換する固有鍵変換手段を備える暗号化固有鍵作成装置を有し、前記第1認証手段は、前記固有鍵を前記固有鍵変換手段へ出力して変換された暗号化固有鍵を受け取り、受け取った暗号化固有鍵を前記アクセス装置へ伝送し、前記第2認証手段は、記録媒体から伝送された暗号化固有鍵に前記第1暗号の逆処理を行う第1復号を施して固有鍵を生成するように構成してもよい。

## 【0010】

ここで、前記第1認証手段は、あらかじめ複数の第1鍵を有し、前記複数の第1鍵のうち一つの第2鍵の選択を受け付け、前記第2鍵を用いて、前記固有鍵に第1暗号を施して暗号化固有鍵を生成して伝送し、前記第2認証手段は、あらかじめ複数の第1鍵を有し、前記複数の第1鍵から前記第2鍵の選択を受け付け、前記第2鍵を用いて、前記伝送された暗号化固有鍵に、前記第1暗号の逆変換を行う第1復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

## 【0011】

また、本発明は、アクセス装置と接続された状態で、前記アクセス装置との間で機器認証と暗号化された著作物の転送とを行う記録媒体であって、記録媒体毎に異なる固有鍵を記憶している固有鍵記憶領域と、前記固有鍵を用いて暗号化される著作物を保持するための領域と、アクセス装置が接続されたとき、記録媒体から当該アクセス装置へ固有鍵を秘密伝送する手順を経て、当該アクセス装置との間で機器認証を行う認証手段と、機器認証が成功した場合にのみ、前記固有鍵を用いて暗号化された著作物を受け取り前記領域に書き込み若しくは前記領域に記憶されている暗号化された著作物を読み出して前記アクセス装置へ出力する転送手段とを備えることを特徴とする。

## 【0012】

また、本発明は、固有鍵を有する記録媒体と接続され、前記記録媒体との間で機器認証と暗号化された著作物の転送とを行うアクセス装置であって、記録媒体

から固有鍵を秘密伝送される手順を経て、前記記録媒体との間で機器認証を行う認証手段と、機器認証が成功した場合にのみ、前記機器認証を経て得た固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する転送手段とを備えることを特徴とする。

【0013】

ここで、前記第1認証手段は、第3鍵を用いて前記固有鍵に第1変換を施して変形鍵を生成し、前記第1鍵を用いて、前記変形鍵に第2変換を施して、暗号化固有鍵を生成して伝送し、前記第2認証手段は、前記第1鍵を用いて、前記伝送された暗号化固有鍵に、前記第2変換の逆変換を行う第2逆変換を施して、復号変形鍵を生成し、前記第3鍵を用いて、前記復号変形鍵に、前記第1変換の逆変換を行う第1逆変換を施して、復号固有鍵を生成し、前記復号固有鍵を用いて、前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

【0014】

ここで、前記第1認証手段は、第1鍵を用いて前記固有鍵に第2変換を施して変形鍵を生成し、前記第3鍵を用いて、前記変形鍵に第1変換を施して暗号化固有鍵を生成して伝送し、前記第2認証手段は、前記第3鍵を用いて、前記伝送された暗号化固有鍵に、前記第1変換の逆変換を行う第1逆変換を施して、復号変形鍵を生成し、前記第1鍵を用いて、前記復号変形鍵に、前記第2変換の逆変換を行う第2逆変換を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

【0015】

ここで、前記第1認証手段は、前記第3鍵を用いて、第1鍵に第1変換を施して、変形第1鍵を生成し、前記変形第1鍵を用いて、前記固有鍵に第2変換を施して暗号化固有鍵を生成して伝送し、前記第2認証手段は、前記第3鍵を用いて、第1鍵に第1変換を施して、変形第1鍵を生成し、前記変形第1鍵を用いて、前記伝送された暗号化固有鍵に、前記第2変換の逆変換を行う第2逆変換を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認

証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

【0016】

ここで、前記第1認証手段は、前記第1鍵を用いて、前記固有鍵に第2変換を施して、暗号化固有鍵を生成して伝送し、前記固有鍵に第3鍵を用いて第1変換を施して変形固有鍵を生成し、前記第2認証手段は、前記第1鍵を用いて、前記伝送された暗号化固有鍵に、前記第1鍵を用いて、前記第2変換の逆変換を行う第2逆変換を施して、復号固有鍵を生成し、前記固有鍵に第3鍵を用いて、第1変換を施して、変形復号固有鍵を生成し、前記変形復号固有鍵を用いて、前記記録媒体との間で機器認証を行い、前記転送手段は、前記変形復号固有鍵を用いて著作物の転送を行うように構成してもよい。

【0017】

ここで、前記著作物が、ある論理的若しくは物理的単位毎に1つ以上のデータブロックにより構成されているものとし、前記著作物の各データブロックを暗号化して記録媒体に転送し、若しくは記録媒体から転送された著作物を復号する際に、前記転送手段は、各データブロック固有のデータブロック鍵を生成し、前記機器認証を経て得た固有鍵と、データブロック鍵とを用いて、対応するデータブロックを暗号化して、記録媒体に転送し、若しくは記録媒体から転送されたデータブロックを復号するように構成してもよい。

【0018】

ここで、前記著作物が、1つ以上のファイルに構成されているものとし、前記著作物の各ファイルを暗号化して記録媒体に転送し、若しくは記録媒体から転送された著作物を復号する際に、前記転送手段は、各ファイル固有のファイル鍵を生成し、前記機器認証を経て得た固有鍵と、ファイル鍵を用いて、対応するファイルを暗号化して記録媒体に転送し、若しくは記録媒体から転送されたファイルを復号するように構成してもよい。

【0019】

ここで、前記アクセス装置は、さらに、操作者からユーザ鍵の入力を受け付けるユーザ鍵受付手段と、前記入力を受け付けられたユーザ鍵と、記憶媒体から秘



密伝送された固有鍵とを基にして、変形鍵を生成する変形鍵生成手段とを有し、前記転送手段は、機器認証が成功した場合にのみ、前記生成された変形鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号するように構成してもよい。

【0020】

【発明の実施の形態】

本発明に係る一つの実施の形態としてのデジタル著作物保護システム100について説明する。

# 1. デジタル著作物保護システム100の構成

デジタル著作物保護システム100は、図1のブロック図に示すように、メモリカード200、メモリカードライタ300、メモリカードリーダー400から構成される。

【0021】

メモリカード200は、図2に示すように、メモリカード挿入口301から挿入され、メモリカードライタ300に装着される。また、メモリカードライタ300は、メモリカードライタ挿入口501から挿入され、パーソナルコンピュータ500に装着される。メモリカードライタ300は、パーソナルコンピュータ500を介して通信回線10により外部と接続されている。

【0022】

パーソナルコンピュータ500は、ディスプレイ503、キーボード504、スピーカ502、図示していないプロセッサ、RAM、ROM、ハードディスク装置を備えている。

メモリカード200は、メモリカードリーダー400に装着される。メモリカード200は、図3に示すように、メモリカード挿入口403から挿入されて、メモリカードリーダー400の一つの実施例としてのヘッドホンステレオ401に装着される。ヘッドホンステレオ401は、上面に操作ボタン404a、404b、404c、404dが配置され、側面にメモリカード挿入口403を有し、別の側面にヘッドホン402が接続されている。

## 1. 1 メモリカード200の構成

メモリカード200は、図4に示すように、マスタ鍵記憶部210、メディア固有鍵記憶部220、変換部230、メディア固有鍵情報記憶部240、装置鍵記憶部221、逆変換部222、装置鍵情報記憶部223、相互認証部250、暗号化著作物記憶部260、通信部270、制御部280から構成される。

### 【0023】

メモリカード200がメモリカードライター300に装着されると、通信部270は、メモリカードライター300の後述する通信部340と接続される。

メモリカード200がメモリカードリーダー400に装着されると、通信部270は、メモリカードリーダー400の後述する通信部440と接続される。

## 1. 1. 1 マスタ鍵記憶部210

マスタ鍵記憶部210は、あらかじめ一つのマスタ鍵Mkを記憶している。マスタ鍵Mkは、56ビットのビット列からなる。マスタ鍵は、デジタル著作物運用システム毎に異なる。さらに、特定のデジタル著作物運用システム用メモリカードを製造するすべてのメーカーにより製造されたすべてのメモリカードのマスタ鍵記憶部には、同じマスタ鍵が記憶されている。

### 【0024】

ここで、デジタル著作物運用システムとは、例えば、A社、B社、C社の3者が共同で運営し、音楽を配信する音楽配信システムであり、また、X社、Y社、Z社が共同で運営する映画レンタルシステムである。

## 1. 1. 2 メディア固有鍵記憶部220

メディア固有鍵記憶部220は、あらかじめ一つの固有鍵Kiを記憶している。固有鍵Kiは、56ビットのビット列からなる。固有鍵は、メモリカード毎に異なる。固有鍵は、メモリカード毎に異なるメモリカードの製造番号と、その都度生成される乱数とに、所定の演算を施して、例えば加算を施して算出される。

### 1. 1. 3 変換部230

変換部230は、メディア固有鍵記憶部220に記憶されている固有鍵 $K_i$ を読み出し、マスタ鍵記憶部210に記憶されているマスタ鍵 $M_k$ を読み出す。

【0025】

変換部230は、DES（データ暗号化規格、Data Encryption Standard）により規格されている暗号アルゴリズム $E_1$ をあらかじめ記憶している。

ここで、DESにより規格されている暗号アルゴリズム $E_1$ は、暗号鍵は56ビットであり、平文及び暗号文の長さは64ビットである。なお、この実施の形態において、暗号アルゴリズム及び復号アルゴリズムは、特に断らない限り、DESにより規格されているアルゴリズムであり、暗号鍵及び復号鍵は56ビットであり、平文及び暗号文の長さは64ビットである。

【0026】

変換部230は、読み出した固有鍵 $K_i$ に暗号アルゴリズム $E_1$ を施して暗号化固有鍵 $J_i$ を生成する。このとき、前記読み出したマスタ鍵 $M_k$ を暗号アルゴリズム $E_1$ の鍵とする。生成された暗号化固有鍵 $J_i$ は式1に示すように表現できる。

$$(式1) \quad J_i = E_1 (M_k, K_i)$$

なお、この明細書において、鍵 $K$ を用いて、平文 $M$ に対して、暗号アルゴリズム $E$ を施し、暗号文 $C$ を生成するとき、式2に示すように表現することとする。

$$(式2) \quad C = E (K, M)$$

また、鍵 $K$ を用いて、前記生成された暗号文 $C$ に対して、復号アルゴリズム $D$ を施して、前記平文 $M$ を生成するとき、式3に示すように表現することとする。

$$(式3) \quad M = D (K, C)$$

このように、鍵 $K$ を用いて、平文 $M$ に対して、暗号アルゴリズム $E$ を施し暗号文 $C$ を生成し、生成された暗号文 $C$ に対して、復号アルゴリズム $D$ を施して、前記平文 $M$ と同一の平文が生成されるとき、暗号アルゴリズム $E$ と復号アルゴリズム $D$ との関係を式4に示すように表現することとする。

$$(式4) \quad E = \text{crypt} (D)$$

変換部 230 は、生成した暗号化固有鍵  $J_i$  をメディア固有鍵情報記憶部 240 へ出力する。

#### 1. 1. 4 メディア固有鍵情報記憶部 240

メディア固有鍵情報記憶部 240 は、変換部 230 から、暗号化固有鍵  $J_i$  を受け取り、受け取った暗号化固有鍵  $J_i$  を記憶する。

#### 1. 1. 5 相互認証部 250

相互認証部 250 は、乱数発生部 251、暗号部 252、復号部 253、相互認証制御部 254 から構成される。

##### (1) 乱数発生部 251

乱数発生部 251 は、乱数  $R_2$  を生成する。乱数  $R_2$  は、64 ビットのビット列からなる。乱数発生部 251 は、生成した乱数  $R_2$  を通信部 270 と相互認証制御部 254 とへ出力する。

##### (2) 暗号部 252

暗号部 252 は、通信部 270 から乱数  $R_1$  を受け取る。

【0027】

暗号部 252 は、メディア固有鍵記憶部 220 から固有鍵  $K_i$  を読み出す。

暗号部 252 は、DES により規格されている暗号アルゴリズム  $E_2$  をあらかじめ記憶している。

暗号部 252 は、受け取った乱数  $R_1$  に暗号アルゴリズム  $E_2$  を施して暗号化乱数  $S_1$  を生成する。このとき、前記読み出した固有鍵  $K_i$  を暗号アルゴリズム  $E_2$  の鍵とする。生成された暗号化乱数  $S_1$  は式 5 に示すように表現できる。

$$(式 5) \quad S_1 = E_2 (K_i, R_1)$$

暗号部 252 は、生成した暗号化乱数  $S_1$  を通信部 270 へ出力する。

##### (3) 復号部 253

復号部 253 は、通信部 270 から暗号化乱数 S2 を受け取り、装置鍵記憶部 221 から装置鍵 A' j を読み出す。

【0028】

復号部 253 は、DES により規格されている復号アルゴリズム D2 をあらかじめ記憶している。

復号部 253 は、受け取った暗号化乱数 S2 に復号アルゴリズム D2 を施して乱数 R' 2 を生成する。このとき、前記読み出した装置鍵 A' j を復号アルゴリズム D2 の鍵とする。生成された乱数 R' 2 は式 6 に示すように表現できる。

$$\begin{aligned} \text{(式 6)} \quad R' 2 &= D2 (A' j, S2) \\ &= D2 (A' j, E2 (A j, R2)) \end{aligned}$$

復号部 253 は、生成した乱数 R' 2 を相互認証制御部 254 へ出力する。

#### (4) 相互認証制御部 254

相互認証制御部 254 は、復号部 253 から乱数 R' 2 を受け取る。また、相互認証制御部 254 は、乱数発生部 251 から乱数 R2 を受け取る。

【0029】

相互認証制御部 254 は、復号部 253 から受け取った乱数 R' 2 と、乱数発生部 251 から受け取った乱数 R2 とを比較し、乱数 R' 2 と乱数 R2 とが一致すれば、メモリカード 200 が装着されたメモリカードライタ 300 又はメモリカードリーダー 400 が正しい装置であると認証し、乱数 R' 2 と乱数 R2 とが一致していなければ、メモリカード 200 が装着されたメモリカードライタ 300 又はメモリカードリーダー 400 が不正な装置であるとみなす。

【0030】

相互認証制御部 254 は、メモリカードライタ 300 又はメモリカードリーダー 400 が正しい装置であるか、不正な装置であるかを示す認証信号を制御部 280 へ出力する。

#### 1. 1. 6 暗号化著作物記憶部 260

暗号化著作物記憶部 260 は、記憶媒体として半導体メモリを有する。

【0031】

暗号化著作物記憶部 260 は、通信部 270 から暗号化部分著作物  $F_i$  ( $i = 1, 2, 3, \dots$ ) を受け取り、受け取った暗号化部分著作物  $F_i$  ( $i = 1, 2, 3, \dots$ ) を記憶する。

1. 1. 7 通信部 270

通信部 270 は、メディア固有鍵情報記憶部 240 から暗号化固有鍵  $J_i$  を読み出し、読み出した暗号化固有鍵  $J_i$  をメモリカードライタ 300 の通信部 340 又はメモリカードリーダー 400 の通信部 440 へ出力する。

【0032】

通信部 270 は、メモリカードライタ 300 の通信部 340 から又はメモリカードリーダー 400 の通信部 440 から乱数  $R_1$  を受け取り、受け取った乱数  $R_1$  を相互認証部 250 の暗号部 252 へ出力する。

通信部 270 は、暗号部 252 から暗号化乱数  $S_1$  を受け取り、受け取った暗号化乱数  $S_1$  をメモリカードライタ 300 の通信部 340 又はメモリカードリーダー 400 の通信部 440 へ出力する。

【0033】

通信部 270 は、メモリカードライタ 300 の通信部 340 又はメモリカードリーダー 400 の通信部 440 から、暗号化装置鍵  $B_j$  を受け取り、受け取った暗号化装置鍵  $B_j$  を装置鍵情報記憶部 223 へ出力する。

通信部 270 は、乱数発生部 251 から乱数  $R_2$  を受け取り、受け取った乱数  $R_2$  をメモリカードライタ 300 の通信部 340 又はメモリカードリーダー 400 の通信部 440 へ出力する。

【0034】

通信部 270 は、メモリカードライタ 300 の通信部 340 又はメモリカードリーダー 400 の通信部 440 から暗号化乱数  $S_2$  を受け取り、受け取った暗号化乱数  $S_2$  を相互認証部 250 の復号部 253 へ出力する。

通信部 270 は、制御部 280 から通信中止信号を受け取ると、メモリカードライタ 300 の通信部 340 又はメモリカードリーダー 400 の通信部 440 との

通信を中止する。

【0035】

通信部 270 は、メモリカードライタ 300 の通信部 340 から暗号化部分著作物  $F_i$  ( $i = 1, 2, 3, \dots$ ) を受け取り、受け取った暗号化部分著作物  $F_i$  ( $i = 1, 2, 3, \dots$ ) を暗号化著作物記憶部 260 へ出力する。

通信部 270 は、暗号化著作物記憶部 260 から暗号化著作物を読み出し、読み出した暗号化著作物をメモリカードリーダー 400 の通信部 440 へ出力する。

#### 1. 1. 8 装置鍵情報記憶部 223

装置鍵情報記憶部 223 は、通信部 270 から暗号化装置鍵  $B_j$  を受け取り、受け取った暗号化装置鍵  $B_j$  を記憶する。

#### 1. 1. 9 逆変換部 222

逆変換部 222 は、装置鍵情報記憶部 223 から暗号化装置鍵  $B_j$  を読み出し、マスタ鍵記憶部 210 に記憶されているマスタ鍵  $M_k$  を読み出す。

【0036】

逆変換部 222 は、DES により規格されている復号アルゴリズム  $D3$  をあらかじめ記憶している。

逆変換部 222 は、読み出した暗号化装置鍵  $B_j$  に復号アルゴリズム  $D3$  を施して装置鍵  $A'_j$  を生成する。このとき、前記読み出したマスタ鍵  $M_k$  を復号アルゴリズム  $D3$  の鍵とする。生成された装置鍵  $A'_j$  は式 7 に示すように表現できる。

$$\begin{aligned} \text{(式 7)} \quad A'_j &= D3 (M_k, B_j) \\ &= D3 (M_k, E3 (M_k, A_j)) \end{aligned}$$

逆変換部 222 は、生成した装置鍵  $A'_j$  を装置鍵記憶部 221 へ出力する。

#### 1. 1. 10 装置鍵記憶部 221

装置鍵記憶部 221 は、逆変換部 222 から出力された装置鍵  $A'_j$  を記憶する。

#### 1. 1. 11 制御部 280

制御部 280 は、相互認証制御部 254 からメモリカード 200 が装着されたメモリカードライタ 300 又はメモリカードリーダ 400 が正しい装置であるか、不正な装置であるかを示す認証信号を受け取る。

【0037】

制御部 280 は、受け取った認証信号が不正な装置であることを示す場合には、メモリカードライタ 300 又はメモリカードリーダ 400 との通信を中止する通信中止信号を通信部 270 へ出力する。

1. 2 メモリカードライタ 300 の構成

メモリカードライタ 300 は、図 5 に示すように、装置鍵記憶部 310、変換部 311、装置鍵情報記憶部 312、マスタ鍵記憶部 313、メディア固有鍵情報記憶部 320、逆変換部 321、メディア固有鍵記憶部 323、相互認証部 330、通信部 340、制御部 350、暗号部 360、著作物記憶部 370、著作物取得部 380 から構成される。

【0038】

著作物取得部 380 は、通信回線 10 を経由して外部と接続されている。

1. 2. 1 装置鍵記憶部 310

装置鍵記憶部 310 は、あらかじめ一つの装置鍵  $A_j$  を記憶している。装置鍵  $A_j$  は、56 ビットのビット列からなる。装置鍵は、メモリカードライタ毎に異なる。装置鍵は、メモリカードライタ毎に異なるメモリカードライタの製造番号と、その都度生成される乱数とに、所定の演算を施して、例えば加算を施して算出される。

1. 2. 2 変換部 311

変換部 311 は、装置鍵記憶部 310 に記憶されている装置鍵  $A_j$  を読み出し、マスタ鍵記憶部 313 に記憶されているマスタ鍵  $M_k$  を読み出す。

【0039】

変換部 311 は、DES により規格されている暗号アルゴリズム E3 をあらか



じめ記憶している。

メモ리카ード 200 の逆変換部 222 に記憶されている復号アルゴリズム D3 と暗号アルゴリズム E3 との間には、式 8 に示す関係がある。

$$(式 8) \quad E3 = \text{crypt} (D3)$$

変換部 311 は、読み出した装置鍵 A<sub>j</sub> に暗号アルゴリズム E3 を施して暗号化装置鍵 B<sub>j</sub> を生成する。このとき、前記読み出したマスタ鍵 M<sub>k</sub> を暗号アルゴリズム E3 の鍵とする。生成された暗号化装置鍵 B<sub>j</sub> は式 9 に示すように表現できる。

$$(式 9) \quad B_j = E3 (M_k, A_j)$$

変換部 311 は、生成した暗号化装置鍵 B<sub>j</sub> を装置鍵情報記憶部 312 へ出力する。

#### 1. 2. 3 装置鍵情報記憶部 312

装置鍵情報記憶部 312 は、変換部 311 から暗号化装置鍵 B<sub>j</sub> を受け取り、受け取った暗号化装置鍵 B<sub>j</sub> を記憶する。

#### 1. 2. 4 マスタ鍵記憶部 313

マスタ鍵記憶部 313 は、あらかじめ一つのマスタ鍵 M<sub>k</sub> を記憶している。マスタ鍵 M<sub>k</sub> は、メモ리카ード 200 のマスタ鍵記憶部 210 が記憶しているマスタ鍵と同じである。

#### 1. 2. 5 メディア固有鍵情報記憶部 320

メディア固有鍵情報記憶部 320 は、通信部 340 から暗号化固有鍵 J<sub>i</sub> を受け取り、受け取った暗号化固有鍵 J<sub>i</sub> を記憶する。

#### 1. 2. 6 逆変換部 321

逆変換部 321 は、メディア固有鍵情報記憶部 320 に記憶されている暗号化固有鍵 J<sub>i</sub> を読み出し、マスタ鍵記憶部 313 に記憶されているマスタ鍵 M<sub>k</sub> を読み出す。

【0040】

逆変換部 321 は、DES により規格されている復号アルゴリズム D1 をあらかじめ記憶している。

メモ리카ード 200 の変換部 230 に記憶されている暗号アルゴリズム E1 と復号アルゴリズム D1 との間には、式 10 に示す関係がある。

$$(式 10) \quad E1 = \text{crypt} (D1)$$

逆変換部 321 は、読み出した暗号化固有鍵 Ji に復号アルゴリズム D1 を施して固有鍵 K' i を生成する。このとき、前記読み出したマスタ鍵 Mk を復号アルゴリズム D1 の鍵とする。生成された固有鍵 K' i は、式 11 に示すように表現できる。

$$(式 11) \quad K' i = D1 (Mk, Ji) \\ = D1 (Mk, E1 (Mk, Ki))$$

逆変換部 321 は、生成した固有鍵 K' i をメディア固有鍵記憶部 323 へ出力する。

1. 2. 7 メディア固有鍵記憶部 323

メディア固有鍵記憶部 323 は、逆変換部 321 から固有鍵 K' i を受け取り、受け取った固有鍵 K' i を記憶する。

1. 2. 8 相互認証部 330

相互認証部 330 は、乱数発生部 331、暗号部 332、復号部 333、相互認証制御部 334 から構成される。

(1) 乱数発生部 331

乱数発生部 331 は、乱数 R1 を生成する。乱数 R1 は、64 ビットのビット列からなる。乱数発生部 331 は、生成した乱数 R1 を通信部 340 へ出力する。また、乱数発生部 331 は、生成した乱数 R1 を相互認証制御部 334 へ出力する。

(2) 暗号部 332

暗号部 332 は、通信部 340 から乱数 R2 を受け取り、装置鍵記憶部 310 から装置鍵 A<sub>j</sub> を読み出す。

【0041】

暗号部 332 は、DES により規格されている暗号アルゴリズム E2 をあらかじめ記憶している。

暗号部 332 は、受け取った乱数 R2 に暗号アルゴリズム E2 を施して暗号化乱数 S2 を生成する。このとき、前記読み出した装置鍵 A<sub>j</sub> を暗号アルゴリズム E2 の鍵とする。生成された暗号化乱数 S2 は式 12 に示すように表現できる。

(式 12)  $S2 = E2 (A_j, R2)$

暗号部 332 は、生成した暗号化乱数 S2 を通信部 340 へ出力する。

(3) 復号部 333

復号部 333 は、通信部 340 から暗号化乱数 S1 を受け取る。

【0042】

復号部 333 は、メディア固有鍵記憶部 323 から固有鍵 K' <sub>i</sub> を読み出す。

復号部 333 は、DES により規格されている復号アルゴリズム D2 をあらかじめ記憶している。

メモリカード 200 の相互認証部 330 の暗号部 252 に記憶されている暗号アルゴリズム E2 と復号アルゴリズム D2 との間には、式 13 に示す関係がある。

(式 13)  $E2 = \text{crypt} (D2)$

復号部 333 は、受け取った暗号化乱数 S1 に復号アルゴリズム D2 を施して乱数 R' <sub>1</sub> を生成する。このとき、前記読み出した固有鍵 K' <sub>i</sub> を復号アルゴリズム D2 の鍵とする。生成された乱数 R' <sub>1</sub> は式 14 に示すように表現できる。

(式 14)  $R' 1 = D2 (K' i, S1)$   
 $= D2 (K' i, E2 (K i, R1))$

復号部 333 は、生成された乱数 R' <sub>1</sub> を相互認証制御部 334 へ出力する。

(4) 相互認証制御部 334

相互認証制御部 334 は、復号部 333 から乱数  $R'1$  を受け取る。また、相互認証制御部 334 は、乱数発生部 331 から乱数  $R1$  を受け取る。

【0043】

相互認証制御部 334 は、復号部 333 から受け取った乱数  $R'1$  と、乱数発生部 331 から受け取った乱数  $R1$  とを比較し、乱数  $R'1$  と乱数  $R1$  とが一致すれば、メモリカードライタ 300 に装着されたメモリカード 200 が正しい装置であると認証し、乱数  $R'1$  と乱数  $R1$  とが一致していなければ、メモリカードライタ 300 に装着されたメモリカード 200 が不正な装置であるとみなす。

【0044】

相互認証制御部 334 は、メモリカードライタ 300 に装着されたメモリカード 200 が正しい装置であるか、不正な装置であるかを示す認証信号を制御部 350 へ出力する。

1. 2. 9 通信部 340

通信部 340 は、メモリカード 200 の通信部 270 から暗号化固有鍵  $Ji$  を受け取り、受け取った暗号化固有鍵  $Ji$  をメディア固有鍵情報記憶部 320 へ出力する。

【0045】

通信部 340 は、乱数発生部 331 から乱数  $R1$  を受け取り、受け取った乱数  $R1$  を、メモリカード 200 の通信部 270 へ出力する。

通信部 340 は、メモリカード 200 の通信部 270 から暗号化乱数  $S1$  を受け取り、受け取った暗号化乱数  $S1$  を相互認証部 330 の復号部 333 へ出力する。

【0046】

通信部 340 は、装置鍵情報記憶部 312 から暗号化装置鍵  $Bj$  を読み出し、読み出した暗号化装置鍵  $Bj$  をメモリカード 200 の通信部 270 へ出力する。

通信部 340 は、メモリカード 200 の通信部 270 から乱数  $R2$  を受け取り、受け取った乱数  $R2$  を相互認証部 330 の暗号部 332 へ出力する。

通信部 340 は、暗号部 332 から暗号化乱数  $S2$  を受け取り、受け取った暗

号化乱数 S2 をメモリカード 200 の通信部 270 へ出力する。

【0047】

通信部 340 は、制御部 350 から通信中止信号を受け取ると、メモリカード 200 の通信部 270 との通信を中止する。

通信部 340 は、暗号部 360 から暗号化部分著作物  $F_i$  ( $i = 1, 2, 3, \dots$ ) を受け取り、受け取った暗号化部分著作物  $F_i$  ( $i = 1, 2, 3, \dots$ ) をメモリカード 200 の通信部 270 へ出力する。

#### 1. 2. 10 制御部 350

制御部 350 は、相互認証制御部 334 からメモリカードライタ 300 に装着されたメモリカード 200 が正しい装置であるか、不正な装置であるかを示す認証信号を受け取る。

【0048】

制御部 350 は、受け取った認証信号が不正な装置であることを示す場合には、メモリカード 200 との通信を中止する通信中止信号を通信部 340 へ出力する。

制御部 350 は、受け取った認証信号が正しい装置であることを示す場合には、著作物取得部 380 に対して、外部からの著作物取得を指示する著作物取得信号を出力する。

#### 1. 2. 11 著作物取得部 380

著作物取得部 380 は、制御部 350 から著作物取得信号を受け取る。

【0049】

著作物取得部 380 は、制御部 350 から著作物取得信号を受け取ると、通信回線 10 を経由して、外部から音楽の著作物を取得し、取得した著作物を著作物記憶部 370 へ出力する。

なお、ここで、著作物は音楽であるとしているが、もちろん音楽に限らない事はいうまでもない。その他の文書、画像、映画なども著作部に含まれる。

### 1. 2. 12 著作物記憶部370

著作物記憶部370は、著作物取得部380から著作物を受け取り、受け取った著作物を記憶する。

### 1. 2. 13 暗号部360

暗号部360は、著作物記憶部370から著作物を読み出し、メディア固有鍵記憶部323から固有鍵 $K' i$ を読み出す。

【0050】

暗号部360は、DESにより規格されている暗号アルゴリズムE2をあらかじめ記憶している。

暗号部360は、読み出した著作物を複数の64ビットのビット列からなる部分著作物 $C i$  ( $i = 1, 2, 3, \dots$ )に分割し、各部分著作物 $C i$  ( $i = 1, 2, 3, \dots$ )に暗号アルゴリズムE2を施して複数の暗号化部分著作物 $F i$  ( $i = 1, 2, 3, \dots$ )を生成する。このとき、前記読み出した固有鍵 $K' i$ を暗号アルゴリズムE2の鍵とする。生成された暗号化部分著作物 $F i$  ( $i = 1, 2, 3, \dots$ )は式15に示すように表現できる。

$$(式15) \quad F i = E2 (K' i, C i) \quad (i = 1, 2, 3, \dots)$$

暗号部360は、生成した暗号化部分著作物 $F i$  ( $i = 1, 2, 3, \dots$ )を通信部340へ出力する。

### 1. 3 メモリカードリーダー400の構成

メモリカードライタ300は、図6に示すように、装置鍵記憶部410、変換部411、装置鍵情報記憶部412、マスタ鍵記憶部413、メディア固有鍵情報記憶部420、逆変換部421、メディア固有鍵記憶部423、相互認証部430、通信部440、制御部450、復号部460、著作物記憶部470、再生部480、操作部490から構成される。

【0051】

装置鍵記憶部410、変換部411、装置鍵情報記憶部412、マスタ鍵記憶部413、メディア固有鍵情報記憶部420、逆変換部421、メディア固有鍵

記憶部 423、相互認証部 430、通信部 440、制御部 450については、それぞれメモリカードリーダー 400の装置鍵記憶部 310、変換部 311、装置鍵情報記憶部 312、マスタ鍵記憶部 313、メディア固有鍵情報記憶部 320、逆変換部 321、メディア固有鍵記憶部 323、相互認証部 330、通信部 340、制御部 350と同等であるので、同等部分の説明は省略し、異なる機能、作用を有する点を中心として説明する。

### 1. 3. 1 制御部 450

制御部 450は、受け取った認証信号が正しい装置であることを示す場合には、復号部 460に対して、通信部 440から出力される暗号化著作物の復号を指示する復号指示を出力する。

### 1. 3. 2 復号部 460

復号部 460は、制御部 450から復号指示を受け取る。

【0052】

復号部 460は、制御部 450から復号指示を受け取ると、通信部 440から暗号化著作物を受け取り、メディア固有鍵記憶部 423から固有鍵  $K' i$  を読み出す。

復号部 460は、DESにより規格されている復号アルゴリズム  $D2$  をあらかじめ記憶している。

【0053】

復号部 460は、受け取った暗号化著作物を複数の64ビットのビット列からなる部分暗号化著作物  $G_i$  ( $i = 1, 2, 3, \dots$ ) に分割し、各部分暗号化著作物  $G_i$  ( $i = 1, 2, 3, \dots$ ) に復号アルゴリズム  $D2$  を施して複数の部分著作物  $H_i$  ( $i = 1, 2, 3, \dots$ ) を生成する。このとき、前記読み出した固有鍵  $K' i$  を復号アルゴリズム  $D2$  の鍵とする。生成された部分著作物  $H_i$  ( $i = 1, 2, 3, \dots$ ) は式 16に示すように表現できる。

$$(式 16) \quad H_i = D2(K' i, G_i) \quad (i = 1, 2, 3, \dots)$$

復号部 460は、生成した部分著作物  $H_i$  ( $i = 1, 2, 3, \dots$ ) を著作

物記憶部470へ出力する。

### 1. 3. 3 著作物記憶部470

著作物記憶部470は、復号部460から部分著作物 $H_i$  ( $i=1, 2, 3, \dots$ )を受け取り、受け取った部分著作物 $H_i$  ( $i=1, 2, 3, \dots$ )を記憶する。

### 1. 3. 4 操作部490

操作部490は、各種のユーザの指示を受け付ける複数の操作ボタンを有している。

#### 【0054】

各種のユーザの指示に対応する操作ボタンが、ユーザにより操作されると、操作された操作ボタンに対応する指示を再生部480に出力する。

### 1. 3. 5 再生部480

再生部480は、操作部490から指示を受け取る。

#### 【0055】

再生部480は、受け取った指示に基づいて、著作物記憶部470に記憶されている音楽の著作物を読み出し、読み出した著作物を再生する。

## 2. デジタル著作物保護システム100の動作

デジタル著作物保護システム100の動作について説明する。

### 2. 1 メモリカード200がメモリカードライター300に装着された場合の概要動作

メモリカード200が、メモリカードライター300に装着された場合の概要動作について、図7に示すフローチャートを用いて説明する。

#### 【0056】

メモリカード200が、メモリカードライター300に装着されると、メモリカ



ードライター300がメモリカード200を認証し（ステップS110）、メモリカードライター300が、メモリカード200は不正な装置であると認識した場合には（ステップS111）、メモリカードライター300とメモリカード200との間で通信を行わず、処理を終了する。

【0057】

メモリカードライター300が、メモリカード200は正しい装置であると認識した場合には（ステップS111）、メモリカード200がメモリカードライター300を認証し（ステップS112）、メモリカード200が、メモリカードライター300は不正な装置であると認識した場合には（ステップS113）、メモリカードライター300とメモリカード200との間で通信を行わず、処理を終了する。

【0058】

メモリカード200が、メモリカードライター300は正しい装置であると認識した場合には（ステップS113）、メモリカードライター300は、外部から著作物を取得し、取得した著作物を暗号化し、メモリカード200へ出力し（ステップS114）、メモリカード200は、暗号化された著作物を記憶する（ステップS115）。

## 2. 2 メモリカード200がメモリカードリーダー400に装着された場合の概要動作

メモリカード200が、メモリカードリーダー400に装着された場合の概要動作について、図8に示すフローチャートを用いて説明する。

【0059】

メモリカード200が、メモリカードリーダー400に装着されると、メモリカードリーダー400がメモリカード200を認証し（ステップS120）、メモリカードリーダー400が、メモリカード200は不正な装置であると認識した場合には（ステップS121）、メモリカードリーダー400とメモリカード200との間で通信を行わず、処理を終了する。

【0060】

メモ리카ードリーダー400が、メモ리카ード200は正しい装置であると認識した場合には（ステップS121）、メモ리카ード200がメモ리카ードリーダー400を認証し（ステップS122）、メモ리카ード200が、メモ리카ードリーダー400は不正な装置であると認識した場合には（ステップS123）、メモ리카ードリーダー400とメモ리카ード200との間で通信を行わず、処理を終了する。

【0061】

メモ리카ード200が、メモ리카ードリーダー400は正しい装置であると認識した場合には（ステップS123）、メモ리카ード200は、暗号化された著作物をメモ리카ードリーダー400へ出力し（ステップS124）、メモ리카ードリーダー400は、メモ리카ード200から出力された暗号された著作物を復号し（ステップS125）、メモ리카ードリーダー400は復号された著作物を再生する（ステップS126）。

2. 3 メモ리카ード200がメモ리카ードライター300に装着された場合の詳細の認証動作

メモ리카ード200が、メモ리카ードライター300に装着された場合の詳細の認証動作について、図9及び図10を用いて説明する。

【0062】

変換部230は、マスタ鍵 $M_k$ を暗号アルゴリズム $E1$ の鍵として、固有鍵 $K_i$ に暗号アルゴリズム $E1$ を施して暗号化固有鍵 $E1(M_k, K_i)$ を生成し（ステップS130）、通信部270は、暗号化固有鍵 $E1(M_k, K_i)$ を通信部340を経由して逆変換部321へ出力し（ステップS131）、逆変換部321は、マスタ鍵 $M_k$ を復号アルゴリズム $D1$ の鍵として、暗号化固有鍵 $E1(M_k, K_i)$ に復号アルゴリズム $D1$ を施して固有鍵 $K'_i = D1(M_k, E1(M_k, K_i))$ を生成し（ステップS132）、乱数発生部331は、乱数 $R_1$ を生成し（ステップS133）、通信部340は、生成された乱数 $R_1$ を通信部270を経由して暗号部252へ出力し（ステップS134）、暗号部252

は、固有鍵 $K_i$ を暗号アルゴリズム $E2$ の鍵として、乱数 $R1$ に暗号アルゴリズム $E2$ を施して暗号化乱数 $E2(K_i, R1)$ を生成し(ステップS135)、通信部270は、通信部340を経由して暗号化乱数 $E2(K_i, R1)$ を復号部333へ出力し(ステップS136)、復号部333は、固有鍵 $K'_i$ を復号アルゴリズム $D2$ の鍵として、暗号化乱数 $E2(K_i, R1)$ に復号アルゴリズム $D2$ を施して、 $D2(K'_i, E2(K_i, R1))$ を生成し(ステップS137)、相互認証制御部334は、乱数 $R1$ と $D2(K'_i, E2(K_i, R1))$ とを比較し、一致していれば、メモリカード200は正しい装置であると認識し、一致していなければ、メモリカード200は不正な装置であると認識する(ステップS138)。

#### 【0063】

変換部311は、マスタ鍵 $Mk$ を暗号アルゴリズム $E3$ の鍵として、装置鍵 $A_j$ に暗号アルゴリズム $E3$ を施して暗号化装置鍵 $E3(Mk, A_j)$ を生成し(ステップS139)、通信部340は、暗号化装置鍵 $E3(Mk, A_j)$ を通信部270を経由して逆変換部222へ出力し(ステップS140)、逆変換部222は、マスタ鍵 $Mk$ を復号アルゴリズム $D3$ の鍵として、暗号化装置鍵 $E3(Mk, A_j)$ に復号アルゴリズム $D3$ を施して装置鍵 $A'_j = D3(Mk, E3(Mk, A_j))$ を生成し(ステップS141)、乱数発生部251は、乱数 $R2$ を生成し(ステップS142)、通信部270は、生成された乱数 $R2$ を通信部340を経由して暗号部332へ出力し(ステップS143)、暗号部332は、装置鍵 $A_j$ を暗号アルゴリズム $E2$ の鍵として、乱数 $R2$ に暗号アルゴリズム $E2$ を施して暗号化乱数 $E2(A_j, R2)$ を生成し(ステップS144)、通信部340は、通信部270を経由して暗号化乱数 $E2(A_j, R2)$ を復号部253へ出力し(ステップS145)、復号部253は、装置鍵 $A'_j$ を復号アルゴリズム $D2$ の鍵として、暗号化乱数 $E2(A_j, R2)$ に復号アルゴリズム $D2$ を施して、 $D2(A'_j, E2(A_j, R2))$ を生成し(ステップS146)、相互認証制御部254は、乱数 $R2$ と $D2(A'_j, E2(A_j, R2))$ とを比較し、一致していれば、メモリカードライタ300は正しい装置であると認識し、一致していなければ、メモリカードライタ300

は不正な装置であると認識する（ステップ S147）。

### 3. その他の実施の形態

なお、本発明を上記の実施の形態に基づいて説明してきたが、本発明は上記の実施の形態に限定されないのはもちろんである。すなわち、以下のような場合も本発明に含まれる。

#### 3. 1 デジタル著作物保護システム 100a

本発明に係るまた別の実施の形態の一つとしてのデジタル著作物保護システム 100a は、図 11 のブロック図に示すように、メモリカード 200a、メディア固有鍵情報作成装置 600、メモリカードライタ 300、メモリカードリーダー 400 から構成される。

##### 【0064】

メモリカードライタ 300、メモリカードリーダー 400 は、それぞれデジタル著作物保護システム 100 のメモリカードライタ 300、メモリカードリーダー 400 とほぼ同様であるので、説明は省略する。

メモリカード 200a は、メディア固有鍵情報作成装置 600 と接続される。

##### 3. 1. 1 メディア固有鍵情報作成装置 600

メディア固有鍵情報作成装置 600 は、マスタ鍵記憶部 210b、メディア固有鍵記憶部 220b、変換部 230b、メディア固有鍵情報記憶部 240b、通信部 270b から構成される。

##### 【0065】

マスタ鍵記憶部 210b、メディア固有鍵記憶部 220b、変換部 230b、メディア固有鍵情報記憶部 240b については、それぞれメモリカード 200 のマスタ鍵記憶部 210、メディア固有鍵記憶部 220、変換部 230、メディア固有鍵情報記憶部 240 と同様の機能、作用、構成を有しており、以下においてはそれぞれの相違点を中心にして説明する

(1) マスタ鍵記憶部 210b

マスタ鍵記憶部 210b は、マスタ鍵記憶部 210 と同様にあらかじめ一つのマスタ鍵 Mk を記憶している。

(2) メディア固有鍵記憶部 220b

メディア固有鍵記憶部 220b は、通信部 270b から固有鍵 Ki を受け取り、受け取った固有鍵 Ki を記憶する。

(3) 変換部 230b

変換部 230b は、変換部 230 と同様にして、メディア固有鍵記憶部 220b に記憶されている固有鍵 Ki とマスタ鍵記憶部 210a に記憶されているマスタ鍵 Mk を用いて、暗号化固有鍵 Ji を生成し、生成した暗号化固有鍵 Ji をメディア固有鍵情報記憶部 240b へ出力する。

(4) メディア固有鍵情報記憶部 240b

メディア固有鍵情報記憶部 240b は、変換部 230b から、暗号化固有鍵 Ji を受け取り、受け取った暗号化固有鍵 Ji を記憶する。

(5) 通信部 270b

通信部 270b は、メモ리카ード 200a の通信部 270a から固有鍵 Ki を受け取り、受け取った固有鍵 Ki をメディア固有鍵記憶部 220b へ出力する。

【0066】

通信部 270b は、メディア固有鍵情報記憶部 240b から暗号化固有鍵 Ji を読み出し、読み出した暗号化固有鍵 Ji をメモ리카ード 200a の通信部 270a へ出力する。

3. 1. 2 メモ리카ード 200a

メモ리카ード 200a は、この図に示すように、マスタ鍵記憶部 210、メデ

メディア固有鍵記憶部 220、メディア固有鍵情報記憶部 240a、装置鍵記憶部 221、逆変換部 222、装置鍵情報記憶部 223、相互認証部 250、暗号化著作物記憶部 260、通信部 270a、制御部 280 から構成される。

【0067】

メモ리카ード 200a のマスタ鍵記憶部 210、メディア固有鍵記憶部 220、装置鍵記憶部 221、逆変換部 222、装置鍵情報記憶部 223、相互認証部 250、暗号化著作物記憶部 260、制御部 280 は、それぞれ、メモ리카ード 200 のマスタ鍵記憶部 210、メディア固有鍵記憶部 220、装置鍵記憶部 221、逆変換部 222、装置鍵情報記憶部 223、相互認証部 250、暗号化著作物記憶部 260、制御部 280 と同じであるので説明を省略し、メモ리카ード 200a のメディア固有鍵情報記憶部 240a、通信部 270a について、メモ리카ード 200 のメディア固有鍵情報記憶部 240、通信部 270 との相違点を中心に説明する。

(1) メディア固有鍵情報記憶部 240a

メディア固有鍵情報記憶部 240a は、通信部 270a から暗号化固有鍵  $J_i$  を受け取り、受け取った暗号化固有鍵  $J_i$  を記憶する。

(2) 通信部 270a

通信部 270a は、メディア固有鍵記憶部 220 から固有鍵  $K_i$  を読み出し、読み出した固有鍵  $K_i$  をメディア固有鍵情報作成装置 600 の通信部 270b へ出力する。

【0068】

通信部 270a は、メディア固有鍵情報作成装置 600 の通信部 270b から暗号化固有鍵  $J_i$  を受け取り、受け取った暗号化固有鍵  $J_i$  をメディア固有鍵情報記憶部 240a へ出力する。

3. 1. 3 メモ리카ード 200a がメモ리카ードライター 300 に装着された場合の詳細の認証動作

メモリカード200aが、メモリカードライター300に装着された場合の詳細の認証動作について、図9との相違点につき、図12を用いて説明する。

【0069】

認証動作の詳細は、図9に示すステップS139～S147が、図12に示すステップS201～S206に置き換えられたものとなる。

乱数発生部251は、乱数R3を生成し（ステップS201）、通信部270aは、生成された乱数R3を通信部340を経由して暗号部332へ出力し（ステップS202）、暗号部332は、マスタ鍵Mkを暗号アルゴリズムE2の鍵として、乱数R3に暗号アルゴリズムE2を施して暗号化乱数E2（Mk、R3）を生成し（ステップS203）、通信部340は、通信部270を経由して暗号化乱数E2（Mk、R3）を復号部253へ出力し（ステップS204）、復号部253は、マスタ鍵Mkを復号アルゴリズムD2の鍵として、暗号化乱数E2（Mk、R3）に復号アルゴリズムD2を施して、D2（Mk、E2（Mk、R3））を生成し（ステップS205）、相互認証制御部254は、乱数R3とD2（Mk、E2（Mk、R3））とを比較し、一致していれば、メモリカードライター300は正しい装置であると認識し、一致していなければ、メモリカードライター300は不正な装置であると認識する（ステップS206）。

### 3. 1. 4 まとめ

この実施の形態によると、メモリカード200aが使用者に配布、販売される前に、メモリカード200aとメディア固有鍵情報作成装置600とが接続され、メディア固有鍵情報作成装置600により生成された暗号化固有鍵Jiがメモリカード200aに書き込まれる。

【0070】

このように構成することにより、メモリカード200から、変換部230を取り去ることができ、メモリカード200aでは、メモリカード200と比較して回路規模を小さくできるという効果がある。

### 3. 2 別のデジタル著作物保護システム

デジタル著作物保護システム100では、メモリカード200、メモリカードライタ300、メモリカードリーダー400は、同一のマスタ鍵を有し、マスタ鍵を共通鍵暗号アルゴリズム又は共通鍵復号アルゴリズムの鍵としているが、マスタ鍵の代わりに、メモリカード200は公開鍵暗号の一種であるRSA暗号の公開鍵 $K_p$ を有し、メモリカードライタ300、メモリカードリーダー400は、その秘密鍵 $K_s$ を有するとしてもよい。

#### 【0071】

ここで、公開鍵 $K_p$ と秘密鍵 $K_s$ は、次のようにして決定される。 $p$ 、 $q$ をそれぞれ約160桁程度の10進数とし、その積を $n$ とし、整数 $L$ を $p-1$ 及び $q-1$ の最小公倍数とし、数 $e$ 及び $d$ を法 $L$ の下で互いに逆数となる数とする。すなわち、 $e \cdot d = 1 \pmod{L}$ とする。また、公開鍵 $K_p$ を $n$ 及び $e$ とし、秘密鍵 $K_s$ を $d$ とする。変換部においては、入力 $M$ に対して法 $n$ の下で $M^e$  ( $M$ の $e$ 乗)の演算を行って変換結果 $C$ を求め、逆変換部においては、入力 $C$ に対して $C^d$  ( $C$ の $d$ 乗)の演算を行う。法 $n$ の下で $C^d = (M^e)^d = M^{ed} = M$ であるから首尾よく逆変換ができることが分かる。

#### 【0072】

公開鍵 $K_p$ は、上記に示すようにしてあらかじめ別の公開鍵生成装置により生成され、生成された公開鍵 $K_p$ がメモリカード200に送信されている。

(メモリカード200がメモリカードライタ300に装着された場合の詳細の認証動作)

次に、メモリカード200がメモリカードライタ300に装着された場合の詳細の認証動作について図13を用いて説明する。なお、図10と同じ符号を有するステップについては、同じ動作であるので説明を省略する。

#### 【0073】

公開鍵生成装置は、あらかじめメモリカードライタ300から秘密鍵 $K_s$ を読み出し、読み出した秘密鍵 $K_s$ を基にして公開鍵暗号アルゴリズムを用いて、公開鍵 $K_p$ を生成し、生成した公開鍵 $K_p$ をメモリカード200に送信し、メモリカード200は送信された公開鍵 $K_p$ を記憶する(ステップS301)。

変換部230は、公開鍵 $K_p$ を暗号アルゴリズムE4の鍵として、固有鍵 $K_i$



に暗号アルゴリズムE4を施して暗号化固有鍵E4 ( $K_p$ 、 $K_i$ )を生成し(ステップS302)、通信部270は、暗号化固有鍵E4 ( $K_p$ 、 $K_i$ )を通信部340を経由して逆変換部321へ出力し(ステップS303)、逆変換部321は、秘密鍵 $K_s$ を復号アルゴリズムD4の鍵として、暗号化固有鍵E4 ( $K_p$ 、 $K_i$ )に復号アルゴリズムD4を施して固有鍵 $K'_i = D4(K_s, E4(K_p, K_i))$ を生成する(ステップS304)。

【0074】

なお、暗号アルゴリズムE4及び復号復号アルゴリズムD4は楕円暗号によるアルゴリズムである。

公開鍵と秘密鍵がこのように構成されているため、秘密鍵 $d$ から公開鍵 $e$ を計算できない。なぜならば、秘密鍵 $d$ が分かっているとき、これから $e$ を求めるためには法 $L$ が知られていなければならないが、 $L$ は $p-1$ と $q-1$ の最小公倍数であるため、 $p$ と $q$ との積を知っているだけでは求められないからである。このことにより、カードリーダー又はカードライターに存在する秘密鍵 $d$ が仮に暴露されたとしてもこれから公開鍵 $e$ を求めることができないので、メモリカードの偽造が困難であるという効果がある。

### 3. 3 別のデジタル著作物保護システム

上記の「3. 2 別のデジタル著作物保護システム」に示すデジタル著作物保護システムでは、メモリカード200は公開鍵 $K_p$ を有し、メモリカードライター300、メモリカードリーダー400は、秘密鍵 $K_s$ を有するとしているが、また別のデジタル著作物保護システムにおいては、メモリカード200は、公開鍵暗号系的一种である楕円曲線上の回復型署名の秘密鍵 $K_s$ を有し、メモリカードライター300、メモリカードリーダー400は、公開鍵 $K_p$ を有するとしてもよい。ここで、公開鍵 $K_p$ と秘密鍵 $K_s$ は次のようにして決定される。

【0075】

秘密鍵 $K_s$ としてスカラー $x$ が選ばれる。公開鍵 $K_p$ は、楕円曲線上の基点を $G$ とし、 $G+G+\cdots+G$ ( $x$ 回の加算)の点とする。変換処理として秘密鍵 $K_s$ を用いた回復型署名変換を用い、逆変換処理として公開鍵 $K_p$ を用いて回復

型署名検証変換を用いる。なお、回復型署名については、「A message recovery signature scheme equivalent to DSA over elliptic curves」(Atsuko Miyaji 著、Advances in Cryptology- Proceedings of ASIACRYPT'96, Lecture Notes in Computer Science, 1163(1996), Springer-Verlag, 1-14) に記載されているので、説明は省略する。

【0076】

このとき、公開鍵  $K_p$  は、メモリカード 200 が有する秘密鍵  $K_s$  を基にして公開鍵暗号アルゴリズムを用いて、あらかじめ別の公開鍵生成装置により生成され、生成された公開鍵  $K_p$  がメモリカードライタ 300 に送信されている。

変換部 230 は、秘密鍵  $K_s$  を暗号アルゴリズム  $E_4$  の鍵として、固有鍵  $K_i$  に暗号アルゴリズム  $E_4$  を施して暗号化固有鍵  $E_4(K_s, K_i)$  を生成する。また、逆変換部 321 は、公開鍵  $K_p$  を復号アルゴリズム  $D_4$  の鍵として、暗号化固有鍵  $E_4(K_s, K_i)$  に復号アルゴリズム  $D_4$  を施して固有鍵  $K'_i = D_4(K_p, E_4(K_s, K_i))$  を生成する。

【0077】

公開鍵  $K_p$  と秘密鍵  $K_s$  がこのように構成されているので、公開鍵  $K_p$  から秘密鍵  $K_s$  を求めることが、計算量的に非常に困難となる。従って、メモリカードに比べて内部解析の危険性が相対的に高いと思われるメモリライタ又はメモリリーダーに公開鍵を与え、メモリカードに秘密鍵を与える構成が、全体のセキュリティを高める効果を持つ。

【0078】

なお、楕円曲線暗号系のような離散対数問題に安全性の根拠を持つ公開鍵暗号系では、秘密鍵から公開鍵が求められることに注意されたい。

### 3. 4 別のデジタル著作物保護システム

本発明に係るまた別の実施の形態の一つとしてのデジタル著作物保護システム 100c は、図 14、図 15、図 16 のブロック図にそれぞれ示すメモリカード 200c、メモリカードライタ 300c、メモリカードリーダー 400c から構成される。

【0079】

メモリカード200cは、図示していないマスタ鍵選択装置に装着される。また、メモリカードライタ300c、メモリカードリーダー400cは、マスタ鍵選択装置に接続される。

3.4.1 マスタ鍵選択装置

マスタ鍵選択装置にメモリカード200cが装着される場合には、マスタ鍵選択装置は、メモリカード200cの通信部270と接続される。

【0080】

マスタ鍵選択装置とメモリカードライタ300cとが接続される場合には、マスタ鍵選択装置は、メモリカードライタ300cの通信部340と接続される。

マスタ鍵選択装置とメモリカードリーダー400cとが接続される場合には、マスタ鍵選択装置は、メモリカードリーダー400cの通信部440と接続される。

マスタ鍵選択装置は、メモリカード200c、メモリカードライタ300c又はメモリカードリーダー400cと接続される場合に、接続されるメモリカード200cの通信部270、メモリカードライタ300cの通信部340又はメモリカードリーダー400cの通信部440に対してパスワードを出力する。

【0081】

パスワードは、複数のマスタ鍵のうちの一つに対応する。

3.4.2 メモリカード200c

メモリカード200cは、メモリカード200にさらにマスタ鍵選択部215を備える。メモリカード200cのその他の構成要素は、メモリカード200と同様である。以下において、メモリカード200との相違点を中心にして説明する。

【0082】

マスタ鍵記憶部210は、複数のマスタ鍵をあらかじめ記憶している。

メモリカード200cがマスタ鍵選択装置に装着されたとき、メモリカード200cは、マスタ鍵選択装置と通信部270を介して接続される。

通信部 270 は、マスタ鍵選択装置からパスワードを受け取り、受け取ったパスワードをマスタ鍵選択部 215 に出力する。

【0083】

マスタ鍵選択部 215 は、通信部 271 から受け取ったパスワードを用いて、対応する一つのマスタ鍵をマスタ鍵記憶部 210 から選択し、選択したマスタ鍵をマスタ鍵記憶部 210 へ出力する。

マスタ鍵記憶部 210 は、選択されたマスタ鍵に選択されたことを示す選択マークを付し、記憶する。

【0084】

変換部 230、逆変換部 222 は、前記選択マークを付されたマスタ鍵を読み出す。

3. 4. 3 メモリカードライタ 300c、メモリカードリーダー 400c

メモリカードライタ 300c は、メモリカードライタ 300 にさらにマスタ鍵選択部 315 を備える。メモリカードライタ 300c のその他の構成要素は、メモリカードライタ 300 と同様である。

【0085】

マスタ鍵記憶部 313 は、複数のマスタ鍵をあらかじめ記憶している。

メモリカード 200c と同様に、通信部 340 はマスタ鍵選択装置からパスワードを受け取り、マスタ鍵選択部 315 に出力し、マスタ鍵選択部 315 は、受け取ったパスワードを用いて、対応する一つのマスタ鍵をマスタ鍵記憶部 313 から選択し、マスタ鍵記憶部 313 は、選択されたマスタ鍵に選択されたことを示す選択マークを付し、記憶する。

【0086】

変換部 311、逆変換部 321 は、前記選択マークを付されたマスタ鍵を読み出す。

メモリカードリーダー 400c についても、メモリカードライタ 300c と同様である。

### 3. 4. 4 まとめ

本実施の形態が適用される望ましい運用形態においては、運用システムの規格を決定すると同時にマスタ鍵などの秘密情報の秘密性を確保する立場にあり、各製造業者にライセンスの許諾を与えるライセンス組織と、ライセンス組織より許諾を受け、所定の規格の機器を製造し、ユーザに提供する立場にある製造業者と、個々の機器を利用するユーザとの3者が存在する。メモリカード用のマスタ鍵選択装置901とメモリカードライタ用のマスタ鍵選択装置902とメモリカードリーダー用のマスタ鍵選択装置903とのうち、マスタ鍵選択装置901は製造業者の手元にあり、マスタ鍵選択装置902とマスタ鍵選択装置903とはライセンス組織の手元にあって、製造業者には渡されない。

#### 【0087】

従って、製造業者が製造する装置の運用状態においては、メモリカードは複数のマスタ鍵を有しており、そのうちの一つをマスタ鍵選択装置901により選択する。一方、メモリカードライタ又はメモリカードリーダーには、予めライセンス組織がマスタ鍵選択装置901又は902を用いて選択した結果のマスタ鍵だけが記録されている。

#### 【0088】

マスタ鍵は運用システム毎に選ばれる。例えば、A社、B社、C社の3者が共同で運営する音楽配信システムには、マスタ鍵Mk1が用いられ、X社、Y社、Z社が共同で運営する映画レンタルシステムにはマスタ鍵Mk2が用いられる。

このように、装置の製造に当たって厳重なセキュリティ条件を課すことが困難なため、異なる運用システムに異なるマスタ鍵が用いられるので、メモリカードよりも相対的に解析が容易と思われるメモリカードライタ又はメモリカードリーダーを運用システム毎に特化することにより、ある運用システムのマスタ鍵の暴露が他の運用システムに影響を与えない、安全性の高いセキュリティシステムを実現できるという効果がある。

### 3. 5 別のデジタル著作物保護システム

本発明に係るまた別の実施の形態の一つとしてのデジタル著作物保護システム

100dは、図17に示すメモリカード200d、メモリカードライター300d、図示していないメモリカードリーダー400dから構成される。

#### 【0089】

メモリカード200d、メモリカードライター300d、メモリカードリーダー400dは、それぞれ、メモリカード200、メモリカードライター300、メモリカードリーダー400と同様の構成であるので、以下においては、相違点を中心に説明する。

### 3.5.1 メモリカード200d

メモリカード200dは、メモリカード200と比較すると、さらにサブグループ鍵記憶部290d、変換部291dを有している点異なる。また、メモリカード200dのその他の構成要素については、以下に説明がない限りにおいては、メモリカード200の構成要素と同様であり、説明を省略する。

#### (1) サブグループ鍵記憶部290d

サブグループ鍵記憶部290dは、あらかじめ一つのサブグループ鍵Gjkを記憶している。サブグループ鍵Gjkは、56ビットのビット列からなる。

#### 【0090】

1つのデジタル著作物運用システムを複数の団体が運営する場合、これらの団体の数だけ、異なるサブグループ鍵が存在し、これらの異なるサブグループ鍵が、それぞれ前記複数の団体に割り当てられる。

例えば、デジタル著作物運用システムは、音楽を配信する音楽配信システムであり、この音楽配信システムをA社、B社、C社の3者が共同で運営する場合に、3つの異なるサブグループ鍵が存在し、これらの異なる3つのサブグループ鍵が、それぞれA社、B社、C社の3者に割り当てられる。

#### (2) 変換部291d

変換部291dは、サブグループ鍵記憶部290dに記憶されている1つのサブグループ鍵Gjkを読み出し、メディア固有鍵記憶部220に記憶されている1

つの固有鍵  $K_i$  を読み出す。

【0091】

変換部 291d は、読み出した 1 つのサブグループ鍵  $G_{jk}$  と、読み出した 1 つの固有鍵  $K_i$  に対して所定の演算を施して、変形鍵を生成する。

ここで、所定の演算とは、排他的論理和である。

変換部 291d は、生成した変形鍵を変換部 230 へ出力する。

### (3) 変換部 230

変換部 230 は、メディア固有鍵記憶部 220 に記憶されている固有鍵  $K_i$  を読み出し、読み出した固有鍵  $K_i$  に暗号アルゴリズム  $E1$  を施して暗号化固有鍵  $J_i$  を生成する代わりに、変換部 291d より変形鍵を受け取り、受け取った変形鍵に暗号アルゴリズム  $E1$  を施して暗号化固有鍵  $J_i$  を生成する。

## 3. 5. 2 メモリカードライタ 300d

メモリカードライタ 300d は、メモリカードライタ 300 と比較すると、さらにサブグループ鍵記憶部 390d、逆変換部 391d を有している点異なる。また、メモリカードライタ 300d のその他の構成要素については、以下に説明がない限りにおいては、メモリカードライタ 300 の構成要素と同様であり、説明を省略する。

### (1) サブグループ鍵記憶部 390d

サブグループ鍵記憶部 390d は、サブグループ鍵記憶部 290d と同様に、あらかじめ一つのサブグループ鍵  $G_{jk}$  を記憶している。サブグループ鍵  $G_{jk}$  は、56 ビットのビット列からなる。

【0092】

サブグループ鍵  $G_{jk}$  については、サブグループ鍵記憶部 290d に記憶されているサブグループ鍵  $G_{jk}$  と同じであるので、説明を省略する。

### (2) 逆変換部 321

逆変換部 321 は、読み出した暗号化固有鍵  $J_i$  に復号アルゴリズム  $D1$  を施して固有鍵  $K'_i$  を生成し、生成した固有鍵  $K'_i$  をメディア固有鍵記憶部 323 へ出力する代わりに、読み出した暗号化固有鍵  $J_i$  に復号アルゴリズム  $D1$  を施して変形鍵を生成し、生成した変形鍵を逆変換部 391d へ出力する。

### (3) 逆変換部 391d

逆変換部 391d は、サブグループ鍵記憶部 390d に記憶されている 1 つのサブグループ鍵  $G_{jk}$  を読み出し、逆変換部 321 から変形鍵を受け取る。

【0093】

逆変換部 391d は、読み出した 1 つのサブグループ鍵  $G_{jk}$  と、受け取った変形鍵とに対して、変換部 291d で施される所定の演算の逆演算を施し、固有鍵  $K'_i$  を生成する。

逆変換部 391d は、生成した固有鍵  $K'_i$  をメディア固有鍵記憶部 323 へ出力する。

### (4) メディア固有鍵記憶部 323

メディア固有鍵記憶部 323 は、逆変換部 391d から固有鍵  $K'_i$  を受け取り、受け取った固有鍵  $K'_i$  を記憶する。

## 3. 5. 3 メモリカードリーダー 400d

メモリカードリーダー 400d は、メモリカードリーダー 400 と比較すると、さらにサブグループ鍵記憶部 490d、逆変換部 491d を有している点異なる。ここで、サブグループ鍵記憶部 490d、逆変換部 491d は、それぞれサブグループ鍵記憶部 390d、逆変換部 391d と同様であるので、説明を省略する。また、メモリカードリーダー 400d の逆変換部 421 とメディア固有鍵記憶部 423 とは、それぞれメモリカードライタ 300d の逆変換部 321 とメディア固有鍵記憶部 323 と同様であり、メモリカードリーダー 400d のその他の構成要素については、メモリカードリーダー 400 の構成要素と同様であるので、説明を省略する。



### 3. 5. 4 デジタル著作物保護システム 100d の動作

デジタル著作物保護システム 100d の動作について説明する。

#### 【0094】

メモリカード 200d がメモリカードライタ 300d に装着された場合の概要動作及びメモリカード 200d がメモリカードリーダー 400d に装着された場合の概要動作については、デジタル著作物保護システム 100 と同様であるので、説明を省略する。

次に、メモリカード 200d がメモリカードライタ 300d に装着された場合の詳細の認証動作について、図 18 を用いて、デジタル著作物保護システム 100 の場合との相違点を中心に説明する。

#### 【0095】

ステップ S150d において、変換部 291d は、サブグループ鍵記憶部 290d に記憶されている 1 つのサブグループ鍵 Gjk を読み出し、メディア固有鍵記憶部 220 に記憶されている 1 つの固有鍵 Ki を読み出し、読み出した 1 つのサブグループ鍵 Gjk と、読み出した 1 つの固有鍵 Ki とに対して所定の演算を施して、変形鍵を生成する。

#### 【0096】

ステップ S130 において、変換部 230 は、マスタ鍵 Mk を暗号アルゴリズム E1 の鍵として、変形鍵に暗号アルゴリズム E1 を施して暗号化固有鍵 E1 (Mk、Ki) を生成する。

ステップ S132 において、逆変換部 321 は、マスタ鍵 Mk を復号アルゴリズム D1 の鍵として、暗号化固有鍵 E1 (Mk、Ki) に復号アルゴリズム D1 を施して変形鍵を生成する。

#### 【0097】

ステップ S151d において、逆変換部 391d は、サブグループ鍵記憶部 390d に記憶されている 1 つのサブグループ鍵 Gjk を読み出し、逆変換部 321 から変形鍵を受け取り、読み出した 1 つのサブグループ鍵 Gjk と、受け取った変形鍵とに対して、変換部 291d で施される所定の演算の逆演算を施し、固有鍵

$K' i = D1 (Mk, E1 (Mk, Ki))$  を生成する。

【0098】

また、メモリカード200dがメモリカードリーダー400dに装着された場合の詳細の認証動作については、上記と同様であるので、説明を省略する。

### 3.5.5 まとめ

1つのデジタル著作物運用システムを複数の団体が運営する場合、これらの団体の数だけ、異なるサブグループ鍵が存在し、これらの異なるサブグループ鍵が、それぞれ前記複数の団体に割り当てられるので、各団体は、独自のサービスの提供が可能となる。

【0099】

例えば、デジタル著作物運用システムは、音楽を配信する音楽配信システムであり、この音楽配信システムをA社、B社、C社の3者が共同で運営する場合に、3つの異なるサブグループ鍵が存在し、これらの異なる3つのサブグループ鍵が、それぞれA社、B社、C社の3者に割り当てられるので、A社、B社、C社は、それぞれ、独自の音楽配信サービスを提供できるようになる。

【0100】

また、メモリカードの記憶容量は限られているので、メモリカードに記憶できるマスタ鍵の数には制限がある場合が多く、マスタ鍵とサブグループ鍵との組合せにより用いることができる鍵の数を増やすことができるという効果がある。

なお、デジタル著作物保護システム100dにおいて、変換部291dによる変換処理を行わず、変換部230に対してメディア固有鍵記録部220に記憶されている固有鍵を変換させる制御部、及び、逆変換部391dによる逆変換処理を行わず、逆変換部321に対してメディア固有鍵情報記録部320に記憶されている暗号化固有鍵を逆変換させる制御部を設けることにより、各団体毎にサブグループ鍵を割り当てた上で、さらに1つのデジタル著作物運用システムに1つのマスタ鍵を割り当てて、各団体の共通のサービスを提供することもできる。

### 3.6 別のデジタル著作物保護システム

本発明に係るまた別の実施の形態の一つとしてのデジタル著作物保護システム 100e は、図 19 に示すメモリカード 200e、メモリカードライタ 300e、図示していないメモリカードリーダー 400e から構成される。

#### 【0101】

メモリカード 200e、メモリカードライタ 300e、メモリカードリーダー 400e は、それぞれ、メモリカード 200、メモリカードライタ 300、メモリカードリーダー 400 と同様の構成であるので、以下においては、相違点を中心に説明する。

### 3. 6. 1 メモリカード 200e

メモリカード 200e は、メモリカード 200 と比較すると、さらにサブグループ鍵記憶部 290e、変換部 291e を有している点が異なる。また、メモリカード 200e のその他の構成要素については、以下に説明がない限りにおいては、メモリカード 200 の構成要素と同様であり、説明を省略する。

#### (1) サブグループ鍵記憶部 290e

サブグループ鍵記憶部 290e は、あらかじめ一つのサブグループ鍵 Gjk を記憶している。サブグループ鍵 Gjk は、56 ビットのビット列からなる。

#### 【0102】

サブグループ鍵は、サブグループ鍵記憶部 290d のサブグループ鍵と同じであるので、説明は省略する。

#### (2) 変換部 291e

変換部 291e は、サブグループ鍵記憶部 290e に記憶されている 1 つのサブグループ鍵 Gjk を読み出し、メディア固有鍵情報記憶部 240 に記憶されている暗号化固有鍵 Ji を読み出す。

#### 【0103】

変換部 291e は、読み出した 1 つのサブグループ鍵 Gjk と、読み出した 1 つの暗号化固有鍵 Ji とに対して所定の演算を施して、変形鍵を生成する。

ここで、所定の演算とは、変換部 291d で用いられる所定の演算と同じ演算である。

変換部 291e は、生成した変形鍵を通信部 270 へ出力する。

### (3) 通信部 270

通信部 270 は、メディア固有鍵情報記憶部 240 から暗号化固有鍵  $J_i$  を読み出し、読み出した暗号化固有鍵  $J_i$  をメモリカードライタ 300 の通信部 340 又はメモリカードリーダ 400 の通信部 440 へ出力する代わりに、変換部 291e から変形鍵を受け取り、受け取った変形鍵をメモリカードライタ 300e の通信部 340 又はメモリカードリーダ 400e の通信部 440 へ出力する。

## 3. 6. 2 メモリカードライタ 300e

メモリカードライタ 300e は、メモリカードライタ 300 と比較すると、さらにサブグループ鍵記憶部 390e、逆変換部 391e を有している点異なる。また、メモリカードライタ 300e のその他の構成要素については、以下に説明がない限りにおいては、メモリカードライタ 300 の構成要素と同様であり、説明を省略する。

### (1) サブグループ鍵記憶部 390e

サブグループ鍵記憶部 390e は、サブグループ鍵記憶部 290e と同様に、あらかじめ一つのサブグループ鍵  $G_{jk}$  を記憶している。サブグループ鍵  $G_{jk}$  は、56 ビットのビット列からなる。

【0104】

サブグループ鍵  $G_{jk}$  については、サブグループ鍵記憶部 290e に記憶されているサブグループ鍵  $G_{jk}$  と同じであるので、説明を省略する。

### (2) 通信部 340

通信部 340 は、メモリカード 200 の通信部 270 から暗号化固有鍵  $J_i$  を受け取り、受け取った暗号化固有鍵  $J_i$  をメディア固有鍵情報記憶部 320 へ出

力する代わりに、メモ리카ード 200e の通信部 270 から変形鍵を受け取り、受け取った変形鍵を逆変換部 391e へ出力する。

### (3) 逆変換部 391e

逆変換部 391e は、サブグループ鍵記憶部 390e に記憶されている 1 つのサブグループ鍵 Gjk を読み出し、通信部 340 から変形鍵を受け取る。

#### 【0105】

逆変換部 391e は、読み出した 1 つのサブグループ鍵 Gjk と、受け取った変形鍵とに対して、変換部 291e で施される所定の演算の逆演算を施し、暗号化固有鍵 Ji を生成する。

逆変換部 391d は、生成した暗号化固有鍵 Ji をメディア固有鍵情報記憶部 320 へ出力する。

### 3. 6. 3 メモ리카ードリーダー 400e

メモ리카ードリーダー 400e は、メモ리카ードリーダー 400 と比較すると、さらにサブグループ鍵記憶部 490e、逆変換部 491e を有している点が異なる。ここで、サブグループ鍵記憶部 490e、逆変換部 491e は、それぞれサブグループ鍵記憶部 390e、逆変換部 391e と同様であるので、説明を省略する。また、メモ리카ードリーダー 400e の通信部 440 は、メモ리카ードライター 300e の通信部 340 と同様であり、メモ리카ードリーダー 400e のその他の構成要素については、メモ리카ードリーダー 400 の構成要素と同様であるので、説明を省略する。

### 3. 6. 4 デジタル著作物保護システム 100e の動作

デジタル著作物保護システム 100e の動作について説明する。

#### 【0106】

メモ리카ード 200e がメモ리카ードライター 300e に装着された場合の概要動作及びメモ리카ード 200e がメモ리카ードリーダー 400e に装着された場合の概要動作については、デジタル著作物保護システム 100 と同様であるので、

説明を省略する。

次に、メモリカード200eがメモリカードライター300eに装着された場合の詳細の認証動作について、図20を用いて、デジタル著作物保護システム100の場合との相違点を中心に説明する。

#### 【0107】

ステップS150eにおいて、変換部291eは、サブグループ鍵記憶部290eに記憶されている1つのサブグループ鍵Gjkを読み出し、メディア固有鍵情報記憶部240に記憶されている暗号化固有鍵Jiを読み出し、読み出した1つのサブグループ鍵Gjkと、読み出した1つの暗号化固有鍵Jiとに対して所定の演算を施して、変形鍵を生成し、生成した変形鍵を通信部270へ出力する。

#### 【0108】

ステップ130において、通信部270は、変換部291eから変形鍵を受け取り、受け取った変形鍵をメモリカードライター300eの通信部340へ出力し、通信部340は、メモリカード200eの通信部270から変形鍵を受け取り、受け取った変形鍵を逆変換部391eへ出力する。

ステップS151eにおいて、逆変換部391eは、サブグループ鍵記憶部390eに記憶されている1つのサブグループ鍵Gjkを読み出し、通信部340から変形鍵を受け取り、読み出した1つのサブグループ鍵Gjkと、受け取った変形鍵とに対して、変換部291eで施される所定の演算の逆演算を施し、暗号化固有鍵Jiを生成する。

#### 【0109】

また、メモリカード200eがメモリカードリーダー400eに装着された場合の詳細の認証動作については、上記と同様であるので、説明を省略する。

### 3. 6. 5 まとめ

デジタル著作物保護システム100dと同様に、1つのデジタル著作物運用システムを複数の団体が運営する場合、これらの団体の数だけ、異なるサブグループ鍵が存在し、これらの異なるサブグループ鍵が、それぞれ前記複数の団体に割り当てられるので、各団体は、独自のサービスの提供が可能となる。

## 【0110】

また、メモ리카ードの記憶容量は限られているので、メモ리카ードに記憶できるマスタ鍵の数には制限がある場合が多く、マスタ鍵とサブグループ鍵との組合せにより用いることができる鍵の数を増やすことができるという効果がある。

なお、デジタル著作物保護システム100eにおいて、変換部291eによる変換処理を行わず、変換部230に対してメディア固有鍵記録部220に記憶されている固有鍵を変換させる制御部、及び、逆変換部391eによる逆変換処理を行わず、逆変換部321に対してメディア固有鍵情報記録部320に記憶されている暗号化固有鍵を逆変換させる制御部を設けることにより、各団体毎にサブグループ鍵を割り当てた上で、さらに1つのデジタル著作物運用システムに1つのマスタ鍵を割り当てて、各団体の共通のサービスを提供することもできる。

## 3. 7 別のデジタル著作物保護システム

本発明に係るまた別の実施の形態の一つとしてのデジタル著作物保護システム100fは、図21に示すメモ리카ード200f、メモ리카ードライタ300f、図示していないメモ리카ードリーダー400fから構成される。

## 【0111】

メモ리카ード200f、メモ리카ードライタ300f、メモ리카ードリーダー400fは、それぞれ、メモ리카ード200、メモ리카ードライタ300、メモ리카ードリーダー400と同様の構成であるので、以下においては、相違点を中心に説明する。

## 3. 7. 1 メモ리카ード200f

メモ리카ード200fは、メモ리카ード200と比較すると、さらにサブグループ鍵記憶部290f、変換部291fを有している点が異なる。また、メモ리카ード200fのその他の構成要素については、以下に説明がない限りにおいては、メモ리카ード200の構成要素と同様であり、説明を省略する。

## (1) サブグループ鍵記憶部290f

サブグループ鍵記憶部 290 f は、あらかじめ一つのサブグループ鍵 G jk を記憶している。サブグループ鍵 G jk は、56 ビットのビット列からなる。

【0112】

サブグループ鍵は、サブグループ鍵記憶部 290 d のサブグループ鍵と同じであるので、説明は省略する。

## (2) 変換部 291 f

変換部 291 f は、サブグループ鍵記憶部 290 f に記憶されている一つのサブグループ鍵 G jk を読み出し、マスタ鍵記憶部 210 に記憶されているマスタ鍵 M<sub>k</sub> を読み出す。

【0113】

変換部 291 f は、読み出した一つのサブグループ鍵 G jk と、読み出した一つのマスタ鍵 M<sub>k</sub> とに対して所定の演算を施して、変形鍵を生成する。

ここで、所定の演算とは、変換部 291 d で用いられる所定の演算と同じ演算である。

変換部 291 f は、生成した変形鍵を変換部 230 へ出力する。

## (3) 変換部 230

変換部 230 は、マスタ鍵記憶部 210 に記憶されているマスタ鍵 M<sub>k</sub> を読み出し、前記読み出したマスタ鍵 M<sub>k</sub> を暗号アルゴリズム E1 の鍵として、読み出した固有鍵 K<sub>i</sub> に暗号アルゴリズム E1 を施して暗号化固有鍵 J<sub>i</sub> を生成する代わりに、変換部 291 f から変形鍵を受け取り、前記受け取った変形鍵を暗号アルゴリズム E1 の鍵として、読み出した固有鍵 K<sub>i</sub> に暗号アルゴリズム E1 を施して暗号化固有鍵 J<sub>i</sub> を生成する。

## 3. 7. 2 メモリカードライタ 300 f

メモリカードライタ 300 f は、メモリカードライタ 300 と比較すると、さらにサブグループ鍵記憶部 390 f、逆変換部 391 f を有している点が異なる。また、メモリカードライタ 300 f のその他の構成要素については、以下に説



明がない限りにおいては、メモリカードライタ 300 の構成要素と同様であり、説明を省略する。

(1) サブグループ鍵記憶部 390f

サブグループ鍵記憶部 390f は、サブグループ鍵記憶部 290f と同様に、あらかじめ一つのサブグループ鍵 Gjk を記憶している。サブグループ鍵 Gjk は、56 ビットのビット列からなる。

【0114】

サブグループ鍵 Gjk については、サブグループ鍵記憶部 290f に記憶されているサブグループ鍵 Gjk と同じであるので、説明を省略する。

(2) 逆変換部 391f

逆変換部 391f は、サブグループ鍵記憶部 390f に記憶されている 1 つのサブグループ鍵 Gjk を読み出し、マスタ鍵記憶部 313 に記憶されているマスタ鍵 Mk を読み出す。

【0115】

逆変換部 391f は、読み出した 1 つのサブグループ鍵 Gjk と、読み出した 1 つのマスタ鍵 Mk とに対して所定の演算を施して、変形鍵を生成する。

ここで、所定の演算とは、変換部 291d で用いられる所定の演算と同じ演算である。

逆変換部 391f は、生成した変形鍵を逆変換部 321 へ出力する。

(3) 逆変換部 321

逆変換部 321 は、マスタ鍵記憶部 313 に記憶されているマスタ鍵 Mk を読み出し、前記読み出したマスタ鍵 Mk を復号アルゴリズム D1 の鍵として、読み出した暗号化固有鍵 Ji に復号アルゴリズム D1 を施して固有鍵 K' i を生成する代わりに、逆変換部 321 から変形鍵を受け取り、受け取った変形鍵を復号アルゴリズム D1 の鍵として、読み出した暗号化固有鍵 Ji に復号アルゴリズム D1 を施して固有鍵 K' i を生成する。

### 3. 7. 3 メモリカードリーダー 400f

メモリカードリーダー 400f は、メモリカードリーダー 400 と比較すると、さらにサブグループ鍵記憶部 490f、逆変換部 491f を有している点異なる。ここで、サブグループ鍵記憶部 490f、逆変換部 491f は、それぞれサブグループ鍵記憶部 390f、逆変換部 391f と同様であるので、説明を省略する。また、メモリカードリーダー 400f の逆変換部 421 は、メモリカードライタ 300f の逆変換部 321 と同様であり、メモリカードリーダー 400f のその他の構成要素については、メモリカードリーダー 400 の構成要素と同様であるので、説明を省略する。

### 3. 7. 4 デジタル著作物保護システム 100f の動作

デジタル著作物保護システム 100f の動作について説明する。

#### 【0116】

メモリカード 200f がメモリカードライタ 300f に装着された場合の概要動作及びメモリカード 200f がメモリカードリーダー 400f に装着された場合の概要動作については、デジタル著作物保護システム 100 と同様であるので、説明を省略する。

次に、メモリカード 200f がメモリカードライタ 300f に装着された場合の詳細の認証動作について、図 22 を用いて、デジタル著作物保護システム 100 の場合との相違点を中心に説明する。

#### 【0117】

ステップ S150f において、変換部 291f は、サブグループ鍵記憶部 290f に記憶されている 1 つのサブグループ鍵 Gjk を読み出し、マスタ鍵記憶部 210 に記憶されているマスタ鍵 Mk を読み出し、読み出した 1 つのサブグループ鍵 Gjk と、読み出した 1 つのマスタ鍵 Mk とに対して所定の演算を施して、変形鍵を生成し、変換部 291f は、生成した変形鍵を変換部 230 へ出力する。

#### 【0118】

ステップ S130 において、変換部 230 は、変形鍵を暗号アルゴリズム E1

の鍵として、固有鍵 $K_i$ に暗号アルゴリズム $E_1$ を施して暗号化固有鍵 $E_1(M_k, K_i)$ を生成する。

ステップS151fにおいて、逆変換部391fは、サブグループ鍵記憶部390fに記憶されている1つのサブグループ鍵 $G_{jk}$ を読み出し、マスタ鍵記憶部313に記憶されているマスタ鍵 $M_k$ を読み出し、読み出した1つのサブグループ鍵 $G_{jk}$ と、読み出した1つのマスタ鍵 $M_k$ とに対して所定の演算を施して、変形鍵を生成し、生成した変形鍵を逆変換部321へ出力する。

【0119】

ステップS132において、逆変換部321は、変形鍵を復号アルゴリズム $D_1$ の鍵として、暗号化固有鍵 $E_1(M_k, K_i)$ に復号アルゴリズム $D_1$ を施して固有鍵 $K'_i = D_1(M_k, E_1(M_k, K_i))$ を生成する。

また、メモ리카ード200fがメモ리카ードリーダ400fに装着された場合の詳細の認証動作については、上記と同様であるので、説明を省略する。

### 3. 7. 5 まとめ

デジタル著作物保護システム100dと同様に、1つのデジタル著作物運用システムを複数の団体が運営する場合、これらの団体の数だけ、異なるサブグループ鍵が存在し、これらの異なるサブグループ鍵が、それぞれ前記複数の団体に割り当てられるので、各団体は、独自のサービスの提供が可能となる。

【0120】

また、メモ리카ードの記憶容量は限られているので、メモ리카ードに記憶できるマスタ鍵の数には制限がある場合が多く、マスタ鍵とサブグループ鍵との組合せにより用いることができる鍵の数を増やすことができるという効果がある。

なお、デジタル著作物保護システム100fにおいて、変換部291fによる変換処理を行わず、変換部230に対してメディア固有鍵記録部220に記憶されている固有鍵を変換させる制御部、及び、逆変換部391fによる逆変換処理を行わず、逆変換部321に対してメディア固有鍵情報記録部320に記憶されている暗号化固有鍵を逆変換させる制御部を設けることにより、各団体毎にサブグループ鍵を割り当てた上で、さらに1つのデジタル著作物運用システムに1つ

のマスタ鍵を割り当てて、各団体の共通のサービスを提供することもできる。

また、デジタル著作物保護システム 100f においては、マスタ鍵記憶部 210 とマスタ鍵記憶部 313 に同じマスタ鍵が記憶されているとしているが、公開鍵方式を用いて次のようにしてもよい。

#### 【0121】

デジタル著作物保護システム 100f においては、メモリカード 200f は、マスタ鍵記憶部 210 は、秘密鍵としてのマスタ鍵を記憶している。メモリカード 200f は、さらに、変換部 291f により生成される変形鍵から公開鍵を生成する公開鍵生成部を有する。生成した公開鍵はメモリカードライタ 300f にあらかじめ配布される。メモリカードライタ 300f において、暗号部 360 は、前記生成された公開鍵を用いて、著作物を暗号化する。

### 3. 8 別のデジタル著作物保護システム

本発明に係るまた別の実施の形態の一つとしてのデジタル著作物保護システム 100g は、図 23 に示すメモリカード 200g、メモリカードライタ 300g、図示していないメモリカードリーダー 400g から構成される。

#### 【0122】

メモリカード 200g、メモリカードライタ 300g、メモリカードリーダー 400g は、それぞれ、メモリカード 200、メモリカードライタ 300、メモリカードリーダー 400 と同様の構成であるので、以下においては、相違点を中心に説明する。

#### 3. 8. 1 メモリカード 200g

メモリカード 200g は、メモリカード 200 と比較すると、さらにサブグループ鍵記憶部 290g、変換部 291g を有している点が異なる。また、メモリカード 200g のその他の構成要素については、以下に説明がない限りにおいては、メモリカード 200 の構成要素と同様であり、説明を省略する。

##### (1) サブグループ鍵記憶部 290g

サブグループ鍵記憶部 290 g は、あらかじめ一つのサブグループ鍵 G jk を記憶している。サブグループ鍵 G jk は、56 ビットのビット列からなる。

【0123】

サブグループ鍵は、サブグループ鍵記憶部 290 d のサブグループ鍵と同じであるので、説明は省略する。

## (2) 変換部 291 g

変換部 291 g は、サブグループ鍵記憶部 290 g に記憶されている一つのサブグループ鍵 G jk を読み出し、メディア固有鍵記憶部 220 に記憶されている固有鍵 K i を読み出す。

【0124】

変換部 291 g は、読み出した一つのサブグループ鍵 G jk と、読み出した一つの固有鍵 K i とに対して所定の演算を施して、変形鍵を生成する。

ここで、所定の演算とは、変換部 291 d で用いられる所定の演算と同じ演算である。

変換部 291 g は、生成した変形鍵を相互認証部 250 の暗号部 252 へ出力する。

## (3) 暗号部 252

暗号部 252 は、メディア固有鍵記憶部 220 から固有鍵 K i を読み出し、前記読み出した固有鍵 K i を暗号アルゴリズム E2 の鍵として、受け取った乱数 R1 に暗号アルゴリズム E2 を施して暗号化乱数 S1 を生成する代わりに、変換部 291 g から変形鍵を受け取り、前記受け取った変形鍵を暗号アルゴリズム E2 の鍵として、受け取った乱数 R1 に暗号アルゴリズム E2 を施して暗号化乱数 S1 を生成する。

## 3. 8. 2 メモリカードライタ 300 g

メモリカードライタ 300 g は、メモリカードライタ 300 と比較すると、さらにサブグループ鍵記憶部 390 g、逆変換部 391 g を有している点が異なる

。また、メモリカードライタ 300g のその他の構成要素については、以下に説明がない限りにおいては、メモリカードライタ 300 の構成要素と同様であり、説明を省略する。

(1) サブグループ鍵記憶部 390g

サブグループ鍵記憶部 390g は、サブグループ鍵記憶部 290g と同様に、あらかじめ一つのサブグループ鍵 Gjk を記憶している。サブグループ鍵 Gjk は、56 ビットのビット列からなる。

【0125】

サブグループ鍵 Gjk については、サブグループ鍵記憶部 290g に記憶されているサブグループ鍵 Gjk と同じであるので、説明を省略する。

(2) 逆変換部 391g

逆変換部 391g は、サブグループ鍵記憶部 390g に記憶されている一つのサブグループ鍵 Gjk を読み出し、メディア固有鍵記憶部 323 に記憶されている固有鍵 K' i を読み出す。

【0126】

逆変換部 391g は、読み出した一つのサブグループ鍵 Gjk と、読み出した一つの固有鍵 K' i とに対して所定の演算を施して、変形鍵を生成する。

ここで、所定の演算とは、変換部 291d で用いられる所定の演算と同じ演算である。

逆変換部 391g は、生成した変形鍵を復号部 333 へ出力する。

(3) 復号部 333

復号部 333 は、メディア固有鍵記憶部 323 から固有鍵 K' i を読み出し、前記読み出した固有鍵 K' i を復号アルゴリズム D2 の鍵として、受け取った暗号化乱数 S1 に復号アルゴリズム D2 を施して乱数 R' 1 を生成する代わりに、逆変換部 391g から変形鍵を受け取り、前記受け取った変形鍵を復号アルゴリズム D2 の鍵として、受け取った暗号化乱数 S1 に復号アルゴリズム D2 を施し

て乱数 R' 1 を生成する。

### 3. 8. 3 メモリカードリーダー 400 g

メモリカードリーダー 400 g は、メモリカードリーダー 400 と比較すると、さらにサブグループ鍵記憶部 490 g、逆変換部 491 g を有している点が異なる。ここで、サブグループ鍵記憶部 490 g、逆変換部 491 g は、それぞれサブグループ鍵記憶部 390 g、逆変換部 391 g と同様であるので、説明を省略する。また、メモリカードリーダー 400 g の復号部 433 は、メモリカードライター 300 g の復号部 333 と同様であり、メモリカードリーダー 400 g のその他の構成要素については、メモリカードリーダー 400 の構成要素と同様であるので、説明を省略する。

### 3. 8. 4 デジタル著作物保護システム 100 g の動作

デジタル著作物保護システム 100 g の動作について説明する。

【0127】

メモリカード 200 g がメモリカードライター 300 g に装着された場合の概要動作及びメモリカード 200 g がメモリカードリーダー 400 g に装着された場合の概要動作については、デジタル著作物保護システム 100 と同様であるので、説明を省略する。

次に、メモリカード 200 g がメモリカードライター 300 g に装着された場合の詳細の認証動作について、図 24 を用いて、デジタル著作物保護システム 100 の場合との相違点を中心に説明する。

【0128】

ステップ S150 g において、変換部 291 g は、サブグループ鍵記憶部 290 g に記憶されている 1 つのサブグループ鍵 Gjk を読み出し、メディア固有鍵記憶部 220 に記憶されている固有鍵 Ki を読み出し、読み出した 1 つのサブグループ鍵 Gjk と、読み出した 1 つの固有鍵 Ki とに対して所定の演算を施して、変形鍵を生成し、生成した変形鍵を相互認証部 250 の暗号部 252 へ出力する。

【0129】

ステップ S135 において、暗号部 252 は、変換部 291 g から変形鍵を受け取り、前記受け取った変形鍵を暗号アルゴリズム E2 の鍵として、受け取った乱数 R1 に暗号アルゴリズム E2 を施して暗号化乱数 S1 を生成する。

ステップ S151 g において、逆変換部 391 g は、サブグループ鍵記憶部 390 g に記憶されている 1 つのサブグループ鍵 Gjk を読み出し、メディア固有鍵記憶部 323 に記憶されている固有鍵 K' i を読み出し、読み出した 1 つのサブグループ鍵 Gjk と、読み出した 1 つの固有鍵 K' i とに対して所定の演算を施して、変形鍵を生成し、生成した変形鍵を復号部 333 へ出力する。

【0130】

ステップ S137 において、復号部 333 は、逆変換部 391 g から変形鍵を受け取り、前記受け取った変形鍵を復号アルゴリズム D2 の鍵として、受け取った暗号化乱数 S1 に復号アルゴリズム D2 を施して乱数 R' 1 を生成する。

また、メモリカード 200 g がメモリカードリーダー 400 g に装着された場合の詳細の認証動作については、上記と同様であるので、説明を省略する。

### 3. 8. 5 まとめ

デジタル著作物保護システム 100 d と同様に、1 つのデジタル著作物運用システムを複数の団体が運営する場合、これらの団体の数だけ、異なるサブグループ鍵が存在し、これらの異なるサブグループ鍵が、それぞれ前記複数の団体に割り当てられるので、各団体は、独自のサービスの提供が可能となる。

【0131】

また、メモリカードの記憶容量は限られているので、メモリカードに記憶できるマスタ鍵の数には制限がある場合が多く、マスタ鍵とサブグループ鍵との組合せにより用いることができる鍵の数を増やすことができるという効果がある。

なお、デジタル著作物保護システム 100 g において、変換部 291 g による変換処理を行わず、変換部 230 に対してメディア固有鍵記録部 220 に記憶されている固有鍵を変換させる制御部、及び、逆変換部 391 g による逆変換処理を行わず、逆変換部 321 に対してメディア固有鍵情報記録部 320 に記憶されている暗号化固有鍵を逆変換させる制御部を設けることにより、各団体毎にサブ



グループ鍵を割り当てた上で、さらに1つのデジタル著作物運用システムに1つのマスタ鍵を割り当てて、各団体の共通のサービスを提供することもできる。

### 3. 9 別のデジタル著作物保護システム

本発明に係るまた別の実施の形態の一つとしてのデジタル著作物保護システム100hは、図25及び図26に示すメモリカード200、メモリカードライタ300h、メモリカードリーダ400hから構成される。

#### 【0132】

メモリカード200は、デジタル著作物保護システム100のメモリカード200と同じであるので、説明を省略する。また、メモリカードライタ300h、メモリカードリーダ400hは、それぞれ、メモリカードライタ300、メモリカードリーダ400と同様の構成であるので、以下においては、相違点を中心に説明する。

#### 3. 9. 1 メモリカードライタ300h

メモリカードライタ300hは、メモリカードライタ300と比較すると、さらに変換部392、ユーザ鍵入力部393を有している点が異なる。また、メモリカードライタ300hのその他の構成要素については、以下に説明がない限りにおいては、メモリカードライタ300の構成要素と同様であり、説明を省略する。

##### (1) ユーザ鍵入力部393

ユーザ鍵入力部393は、キーボードなどの入力装置を含み、ユーザから当該ユーザだけが知っており、ユーザ固有のパスワードであるユーザ鍵の入力を受け付ける。

#### 【0133】

ユーザ鍵は、それぞれのユーザが決定でき、10桁以内の英数字、記号の組合せからなる。

ユーザ鍵入力部393は、ユーザ鍵の入力を受け付けると、入力を受け付けた

ユーザ鍵を変換部392へ出力する。

## (2) 変換部392

変換部392は、メディア固有鍵記憶部323から固有鍵 $K' i$ を読み出し、ユーザ鍵入力部393からユーザ鍵を受け取る。

【0134】

変換部392は、読み出した固有鍵 $K' i$ と、受け取ったユーザ鍵とに対して所定の演算を施して、変形鍵を生成する。ここで、所定の演算とは、排他的論理和である。

変換部392は、生成した変形鍵を暗号部360へ出力する。

## (3) 暗号部360

暗号部360は、メディア固有鍵記憶部323から固有鍵 $K' i$ を読み出し、前記読み出した固有鍵 $K' i$ を暗号アルゴリズムE2の鍵として、読み出した著作物を複数の64ビットのビット列からなる部分著作物 $C i$  ( $i = 1, 2, 3, \dots$ )に分割し、各部分著作物 $C i$  ( $i = 1, 2, 3, \dots$ )に暗号アルゴリズムE2を施して複数の暗号化部分著作物 $F i$  ( $i = 1, 2, 3, \dots$ )を生成する代わりに、変換部392から変形鍵を受け取り、受け取った変形鍵を暗号アルゴリズムE2の鍵として、読み出した著作物を複数の64ビットのビット列からなる部分著作物 $C i$  ( $i = 1, 2, 3, \dots$ )に分割し、各部分著作物 $C i$  ( $i = 1, 2, 3, \dots$ )に暗号アルゴリズムE2を施して複数の暗号化部分著作物 $F i$  ( $i = 1, 2, 3, \dots$ )を生成する。

### 3.9.2 メモリカードリーダー400h

メモリカードリーダー400hは、メモリカードリーダー400と比較すると、さらに変換部492、ユーザ鍵入力部493を有している点異なる。また、メモリカードリーダー400hのその他の構成要素については、以下に説明がない限りにおいては、メモリカードリーダー400の構成要素と同様であり、説明を省略する。

(1) ユーザ鍵入力部 493

ユーザ鍵入力部 493 は、ユーザ鍵入力部 393 と同様に、ユーザからユーザ鍵の入力を受け付け、入力を受け付けたユーザ鍵を変換部 492 へ出力する。

(2) 変換部 492

変換部 492 は、変換部 392 と同様に、メディア固有鍵記憶部 423 から固有鍵  $K' i$  を読み出し、ユーザ鍵入力部 493 からユーザ鍵を受け取り、読み出した固有鍵  $K' i$  と、受け取ったユーザ鍵とに対して所定の演算を施して、変形鍵を生成する。ここで、所定の演算とは、排他的論理和である。

【0135】

変換部 492 は、生成した変形鍵を復号部 460 へ出力する。

(3) 復号部 460

復号部 460 は、メディア固有鍵記憶部 423 から固有鍵  $K' i$  を読み出し、前記読み出した固有鍵  $K' i$  を復号アルゴリズム D2 の鍵として、受け取った暗号化著作物を複数の 64 ビットのビット列からなる部分暗号化著作物  $G_i$  ( $i = 1, 2, 3, \dots$ ) に分割し、各部分暗号化著作物  $G_i$  ( $i = 1, 2, 3, \dots$ ) に復号アルゴリズム D2 を施して複数の部分著作物  $H_i$  ( $i = 1, 2, 3, \dots$ ) を生成する代わりに、変換部 492 から変形鍵を受け取り、受け取った変形鍵を復号アルゴリズム D2 の鍵として、受け取った暗号化著作物を複数の 64 ビットのビット列からなる部分暗号化著作物  $G_i$  ( $i = 1, 2, 3, \dots$ ) に分割し、各部分暗号化著作物  $G_i$  ( $i = 1, 2, 3, \dots$ ) に復号アルゴリズム D2 を施して複数の部分著作物  $H_i$  ( $i = 1, 2, 3, \dots$ ) を生成する。

### 3. 9. 3 デジタル著作物保護システム 100h の動作

デジタル著作物保護システム 100h の動作について説明する。

【0136】

メモ리카ード200がメモ리카ードライター300hに装着された場合の詳細の認証動作、及び、メモ리카ード200がメモ리카ードリーダー400hに装着された場合の詳細の認証動作については、デジタル著作物保護システム100と同じであるので、説明を省略し、メモ리카ード200がメモ리카ードライター300hに装着された場合の概要動作及びメモ리카ード200がメモ리카ードリーダー400hに装着された場合の概要動作について、以下に説明する。

(1)メモ리카ード200がメモ리카ードライター300hに装着された場合の概要動作

メモ리카ード200がメモ리카ードライター300hに装着された場合の概要動作については、図7に示すフローチャートのステップS114の詳細が、デジタル著作物保護システム100の動作と異なるのみであるので、次に、図27に示すフローチャートを用いて、ステップS114の詳細について説明する。

【0137】

ユーザ鍵入力部393は、ユーザからユーザ鍵の入力を受け付け、入力を受け付けたユーザ鍵を変換部392へ出力し(ステップS100h)、変換部392は、メディア固有鍵記憶部323から固有鍵 $K'i$ を読み出し、ユーザ鍵入力部393からユーザ鍵を受け取り、読み出した固有鍵 $K'i$ と、受け取ったユーザ鍵とに対して所定の演算を施して、変形鍵を生成し、生成した変形鍵を暗号部360へ出力し(ステップS101h)、暗号部360は、変換部392から変形鍵を受け取り、受け取った変形鍵を暗号アルゴリズムE2の鍵として、読み出した著作物を複数の64ビットのビット列からなる部分著作物 $Ci$  ( $i=1, 2, 3, \dots$ )に分割し、各部分著作物 $Ci$  ( $i=1, 2, 3, \dots$ )に暗号アルゴリズムE2を施して複数の暗号化部分著作物 $Fi$  ( $i=1, 2, 3, \dots$ )を生成し、生成した暗号化部分著作物 $Fi$ を通信部340へ出力し(ステップS102h)、通信部340は暗号化部分著作物 $Fi$ をメモ리카ード200の通信部270へ出力する(ステップS103h)。

(2)メモ리카ード200がメモ리카ードリーダー400hに装着された場合の概

## 要動作

メモリカード200がメモリカードリーダー400hに装着された場合の概要動作については、図8に示すフローチャートのステップS125の詳細が、デジタル著作物保護システム100の動作と異なるのみであるので、次に、図28に示すフローチャートを用いて、ステップS125の詳細について説明する。

## 【0138】

ユーザ鍵入力部493は、ユーザからユーザ鍵の入力を受け付け、入力を受け付けたユーザ鍵を変換部492へ出力し（ステップS111h）、変換部492は、メディア固有鍵記憶部423から固有鍵 $K' i$ を読み出し、ユーザ鍵入力部493からユーザ鍵を受け取り、読み出した固有鍵 $K' i$ と、受け取ったユーザ鍵とに対して所定の演算を施して、変形鍵を生成し、生成した変形鍵を復号部460へ出力し（ステップS112h）、復号部460は、変換部492から変形鍵を受け取り、受け取った変形鍵を復号アルゴリズムD2の鍵として、受け取った暗号化著作物を複数の64ビットのビット列からなる部分暗号化著作物 $G_i$ （ $i = 1, 2, 3, \dots$ ）に分割し、各部分暗号化著作物 $G_i$ （ $i = 1, 2, 3, \dots$ ）に復号アルゴリズムD2を施して複数の部分著作物 $H_i$ （ $i = 1, 2, 3, \dots$ ）を生成する（ステップS113h）。

## 3.9.5 まとめ

ユーザは、自分で設定したユーザ鍵を用いて著作物を暗号化し、暗号化した著作物を前記ユーザ鍵を用いて復号できるので、ユーザ自身の著作物が他人に解読されず、保護できるという効果がある。

## 3.10 別のデジタル著作物保護システム

本発明に係るまた別の実施の形態の一つとしてのデジタル著作物保護システム100iは、図29及び図30に示すメモリカード200i、メモリカードライター300i、メモリカードリーダー400iから構成される。

## 【0139】

メモリカード200i、メモリカードライター300i、メモリカードリーダー4

00iは、それぞれ、デジタル著作物保護システム100のメモ리카ード200、メモ리카ードライター300、メモ리카ードリーダー400と同様の構成であるので、以下においては、相違点を中心にして説明する。

### 3. 10. 1 メモ리카ードライター300i

メモ리카ードライター300iは、メモ리카ードライター300と比較すると、さらに暗号部365、ファイル鍵生成部366を有している点が異なる。また、メモ리카ードライター300iのその他の構成要素については、以下に説明がない限りにおいては、メモ리카ードライター300の構成要素と同様であり、説明を省略する。

#### (1) 制御部350

制御部350は、著作物取得部380に対して、ファイル毎に、外部からの著作物取得を指示する著作物取得信号を出力し、また、ファイル鍵生成部366に対して、ファイル毎にファイル鍵を生成する生成指示を出力する。

#### (2) 著作物取得部380

著作物取得部380は、1つの著作物をファイルとして取得する。ここで、ファイルとは、一定の規則で集めたデータの集合である。例えば、音楽の著作物の場合は、1曲が1つのファイルに相当する。

#### (3) 著作物記憶部370

著作物記憶部370は、ファイル毎に著作物を記憶する。

#### (4) ファイル鍵生成部366

ファイル鍵生成部366は、制御部350からの生成指示を受けて、56ビットからなるファイル鍵をランダムに生成し、生成したファイル鍵を暗号部365へ出力する。

【0140】

なお、ファイル鍵をランダムに生成しているが、ファイル鍵生成部 366 は、操作者からファイル鍵の入力を受け取るとしてもよい。

#### (5) 暗号部 365

暗号部 365 は、メディア固有鍵記憶部 323 から固有鍵  $K' i$  を読み出し、ファイル鍵生成部 366 より、ファイル鍵を受け取る。

【0141】

暗号部 365 は、DES により規格されている暗号アルゴリズム E5 をあらかじめ記憶している。

暗号部 365 は、受け取ったファイル鍵に暗号アルゴリズム E5 を施して暗号化ファイル鍵を生成する。このとき、前記読み出した固有鍵  $K' i$  を暗号アルゴリズム E5 の鍵とする。

【0142】

暗号部 365 は、生成した暗号化ファイル鍵を通信部 340 へ出力する。

#### (6) 暗号部 360

暗号部 360 は、メディア固有鍵記憶部 323 から固有鍵  $K' i$  を読み出し、前記読み出した固有鍵  $K' i$  を暗号アルゴリズム E2 の鍵とし、読み出した著作物を複数の 64 ビットのビット列からなる部分著作物  $C i$  ( $i = 1, 2, 3, \dots$ ) に分割し、各部分著作物  $C i$  ( $i = 1, 2, 3, \dots$ ) に暗号アルゴリズム E2 を施して複数の暗号化部分著作物  $F i$  ( $i = 1, 2, 3, \dots$ ) を生成する代わりに、暗号部 360 は、ファイル毎に著作物を読み出し、ファイル鍵生成部 366 からファイル鍵を受け取り、受け取ったファイル鍵を暗号アルゴリズム E2 の鍵とし、ファイル毎に読み出した著作物を複数の 64 ビットのビット列からなる部分著作物  $C i$  ( $i = 1, 2, 3, \dots$ ) に分割し、各部分著作物  $C i$  ( $i = 1, 2, 3, \dots$ ) に暗号アルゴリズム E2 を施して複数の暗号化部分著作物  $F i$  ( $i = 1, 2, 3, \dots$ ) を生成する。

#### (7) 通信部 340

通信部340は、さらに、暗号部365から暗号化ファイル鍵を受け取り、受け取った暗号化ファイル鍵を通信部270へ出力する。

### 3. 10. 2 メモリカード200i

メモリカード200iについて、メモリカード200と比較して異なる構成要素について、その相違点を中心に以下に説明する。

#### (1) 通信部270

通信部270は、さらに、通信部340から暗号化ファイル鍵を受け取り、受け取った暗号化ファイル鍵を暗号化著作物記憶部260へ出力する。

##### 【0143】

また、通信部270は、さらに、暗号化著作物記憶部260から暗号化ファイル鍵261を読み出し、読み出した暗号化ファイル鍵を通信部440へ出力する。

。

#### (2) 暗号化著作物記憶部260

暗号化著作物記憶部260は、さらに、通信部270から暗号化ファイル鍵を受け取り、受け取った暗号化ファイル鍵261を記憶する。

##### 【0144】

また、暗号化著作物記憶部260は、通信部270から受け取った暗号化部分著作物Fi (i=1、2、3、・・・)を暗号化ファイル262として記憶する。

。

### 3. 10. 3 メモリカードリーダー400i

メモリカードリーダー400iは、メモリカードリーダー400と比較すると、さらに復号部465を有している点が異なる。また、メモリカードリーダー400iのその他の構成要素については、以下に説明がない限りにおいては、メモリカードリーダー400の構成要素と同様であり、説明を省略する。



(1) 通信部 440

通信部 440 は、さらに、通信部 270 より暗号化ファイル鍵を受け取り、受け取った暗号化ファイル鍵を復号部 465 へ出力する。

(2) 復号部 465

復号部 465 は、メディア固有鍵記憶部 423 から固有鍵  $K' i$  を読み出し、通信部 440 より、暗号化ファイル鍵を受け取る。

【0145】

復号部 465 は、DES により規格されている復号アルゴリズム D5 をあらかじめ記憶している。

ここで、暗号部 365 に記憶されている暗号アルゴリズム E5 と復号アルゴリズム D5 との間には、式 17 に示す関係がある。

(式 17)  $E5 = \text{crypt}(D5)$

復号部 465 は、受け取った暗号化ファイル鍵に復号アルゴリズム D5 を施してファイル鍵を生成する。このとき、前記読み出した固有鍵  $K' i$  を復号アルゴリズム D5 の鍵とする。

【0146】

復号部 465 は、生成したファイル鍵を復号部 460 へ出力する。

(3) 復号部 460

復号部 460 は、メディア固有鍵記憶部 423 から固有鍵  $K' i$  を読み出し、前記読み出した固有鍵  $K' i$  を復号アルゴリズム D2 の鍵として、受け取った暗号化著作物を複数の 64 ビットのビット列からなる部分暗号化著作物  $G_i$  ( $i = 1, 2, 3, \dots$ ) に分割し、各部分暗号化著作物  $G_i$  ( $i = 1, 2, 3, \dots$ ) に復号アルゴリズム D2 を施して複数の部分著作物  $H_i$  ( $i = 1, 2, 3, \dots$ ) を生成する代わりに、復号部 465 からファイル鍵を受け取り、受け取ったファイル鍵を復号アルゴリズム D2 の鍵として、受け取った暗号化著作物を複数の 64 ビットのビット列からなる部分暗号化著作物  $G_i$  ( $i = 1, 2, 3, \dots$ ) に分割し、各部分暗号化著作物  $G_i$  ( $i = 1, 2, 3, \dots$ ) に復

号アルゴリズムD2を施して複数の部分著作物 $H_i$  ( $i=1, 2, 3, \dots$ )を生成する。

### 3. 10. 4 デジタル著作物保護システム100iの動作

デジタル著作物保護システム100iの動作について説明する。

#### 【0147】

メモ리카ード200iがメモ리카ードライター300iに装着された場合の詳細の認証動作、及び、メモ리카ード200iがメモ리카ードリーダー400iに装着された場合の詳細の認証動作については、デジタル著作物保護システム100と同じであるので、説明を省略し、メモ리카ード200iがメモ리카ードライター300iに装着された場合の概要動作及びメモ리카ード200iがメモ리카ードリーダー400iに装着された場合の概要動作について、以下に説明する。

(1) メモ리카ード200iがメモ리카ードライター300iに装着された場合の概要動作

メモ리카ード200iがメモ리카ードライター300iに装着された場合の概要動作については、図7に示すフローチャートのステップS114の詳細が、デジタル著作物保護システム100の動作と異なるのみであるので、次に、図31に示すフローチャートを用いて、ステップS114の詳細について説明する。

#### 【0148】

ファイル鍵生成部366は、制御部350から生成指示を受けて、64ビットからなるファイル鍵をランダムに生成し、生成したファイル鍵を暗号部365へ出力し、暗号部365は、メディア固有鍵記憶部323から固有鍵 $K'_i$ を読み出し、ファイル鍵生成部366より、ファイル鍵を受け取り、前記読み出した固有鍵 $K'_i$ を暗号アルゴリズムE5の鍵として、暗号部365は、受け取ったファイル鍵に暗号アルゴリズムE5を施して暗号化ファイル鍵を生成し、生成した暗号化ファイル鍵を通信部340へ出力する(ステップS100i)。通信部340は、暗号部365から暗号化ファイル鍵を受け取り、受け取った暗号化ファイル鍵を通信部270へ出力する(ステップS101i)。暗号部360は、フ

ファイル鍵生成部 366 からファイル鍵を受け取り、受け取ったファイル鍵を暗号アルゴリズム E2 の鍵とし、読み出した著作物を複数の 64 ビットのビット列からなる部分著作物  $C_i$  ( $i = 1, 2, 3, \dots$ ) に分割し、各部分著作物  $C_i$  ( $i = 1, 2, 3, \dots$ ) に暗号アルゴリズム E2 を施して複数の暗号化部分著作物  $F_i$  ( $i = 1, 2, 3, \dots$ ) を生成する (ステップ S102i)。通信部 340 は、暗号部 360 から複数の暗号化部分著作物を受け取り、受け取った複数の暗号化部分著作物を通信部 270 へ出力する (ステップ S103i)。

(2) メモリカード 200i がメモリカードリーダー 400i に装着された場合の概要動作

通信部 440 は、通信部 270 より暗号化ファイル鍵を受け取り、受け取った暗号化ファイル鍵を復号部 465 へ出力し、復号部 465 は、メディア固有鍵記憶部 423 から固有鍵  $K'_i$  を読み出し、通信部 440 より、暗号化ファイル鍵を受け取り、前記読み出した固有鍵  $K'_i$  を復号アルゴリズム D5 の鍵として、復号部 465 は、受け取った暗号化ファイル鍵に復号アルゴリズム D5 を施してファイル鍵を生成し、生成したファイル鍵を復号部 460 へ出力する (ステップ S111i)。復号部 460 は、復号部 465 からファイル鍵を受け取り、受け取ったファイル鍵を復号アルゴリズム D2 の鍵として、受け取った暗号化著作物を複数の 64 ビットのビット列からなる部分暗号化著作物  $G_i$  ( $i = 1, 2, 3, \dots$ ) に分割し、各部分暗号化著作物  $G_i$  ( $i = 1, 2, 3, \dots$ ) に復号アルゴリズム D2 を施して複数の部分著作物  $H_i$  ( $i = 1, 2, 3, \dots$ ) を生成する (ステップ S112i)。

### 3. 10. 5 まとめ

著作物を形成するファイル毎に、異なるファイル鍵を生成し、生成された異なるファイル鍵でファイル単位の著作物を暗号化するので、ファイルが盗聴されにくくなり、ファイルの安全性が向上するという効果がある。

なお、デジタル著作物保護システム 100i は次のように構成してもよい。

## (1) デジタル著作物保護システム 100 i の変形例 1

図 33 に示すように、メモ리카ード 200 i は、さらに、乱数シード生成部 292 を有し、乱数シード生成部 292 は、乱数の初期値であるシードを生成する。ここで、シードは 64 ビットからなる時刻である。シードは、時刻など値のように時々刻々変化する値が望ましい。乱数シード生成部 292 は、生成したシードを通信部 270 へ出力し、通信部 270 はシードを受け取り、受け取ったシードを通信部 340 へ出力する。通信部 340 はシードを受け取り、受け取ったシードをファイル鍵生成部 366 へ出力する。ファイル鍵生成部 366 は、シードを受け取り、受け取ったシードを用いて、乱数を発生させる。

【0149】

なお、ファイル鍵生成部 366 は、次のようにして乱数を発生させるとしてもよい。

ファイル鍵生成部 366 は、前記受け取ったシードを所定の暗号アルゴリズムを用いて暗号化し、暗号文を生成する。ここで、鍵は所定の鍵を用いる。さらに、ファイル鍵生成部 366 は、生成された暗号文を前記所定の暗号アルゴリズムを用いて、暗号化して暗号文を生成する。この暗号処理を特定回数繰り返し、最後に生成された暗号文を前記乱数とする。

## (2) デジタル著作物保護システム 100 i の変形例 2

図 34 に示すように、メモ리카ード 200 i は、さらに、乱数シード生成部 293 を有し、乱数シード生成部 293 は、乱数シード生成部 293 と同様に、乱数の初期値であるシードを生成する。ここで、シードは 64 ビットからなる時刻である。シードは、時刻など値のように時々刻々変化する値が望ましい。乱数シード生成部 293 は、生成したシードを相互認証部 250 へ出力する。相互認証部 250 は、前記シードを受け取り、受け取ったシードを認証プロセスにより、通信部 270、通信部 340 を経由して、相互認証部 330 へ出力する。相互認証部 330 はシードを受け取り、受け取ったシードをファイル鍵生成部 366 へ出力する。ファイル鍵生成部 366 は、シードを受け取り、受け取ったシードを用いて、乱数を発生させる。

【0150】

次に、上記の認証プロセスの動作の詳細について、図9及び図10に示すフローチャートとの相違点を中心として説明する。

ステップS135において、暗号部252は、乱数シード生成部293からシードSを受け取り、乱数R1とシードSとを結合して、 $(R1 + S)$ を生成し、合計128ビットのビット列とする。暗号部252は、固有鍵 $K_i$ を暗号アルゴリズムE2の鍵として、 $(R1 + S)$ に暗号アルゴリズムE2を施して暗号化乱数E2( $K_i$ 、 $(R1 + S)$ )を生成する。ここで、 $(R1 + S)$ は、128ビットのビット列であるので、64ビットずつの2ブロックに分けて暗号化する。

【0151】

ステップS136において、通信部270は、通信部340を経由して2ブロックの暗号化乱数E2( $K_i$ 、 $(R1 + S)$ )を復号部333へ出力する。

ステップS137において、復号部333は、固有鍵 $K'_i$ を復号アルゴリズムD2の鍵として、暗号化乱数E2( $K_i$ 、 $(R1 + S)$ )に復号アルゴリズムD2を施して、D2( $K'_i$ 、E2( $K_i$ 、 $(R1 + S)$ ))を生成する。復号部333は、D2( $K'_i$ 、E2( $K_i$ 、 $(R1 + S)$ ))を前半の64ビットのビット列と後半の64ビットのビット列に分離する。

【0152】

ステップS138において、相互認証制御部334は、乱数R1と前記前半64ビットのビット列とを比較し、一致していれば、メモリカード200は正しい装置であると認識し、一致していなければ、メモリカード200は不正な装置であると認識する。また、一致している場合には、相互認証制御部334は、後半の64ビットのビット列がシードSであると判断し、シードSをファイル鍵生成部366へ出力する。

【0153】

なお、上記において、乱数R1とシードSとを結合して、 $(R1 + S)$ を生成するとしているが、乱数R1を32ビットずつの前半ビット列と後半ビット列に分離し、シードSを32ビットずつの前半ビット列と後半ビット列に分離し、乱数R1の前半ビット列と、シードSの前半ビット列と、乱数R1の後半

ビット列、シードSの後半ビット列とをこの順に結合するとしてもよい。

### (3) デジタル著作物保護システム100iの変形例3

前記著作物が、ある論理的若しくは物理的単位毎に1つ以上のデータブロックにより構成されているものとし、前記著作物の各データブロックを暗号化して記録媒体に転送し、若しくは記録媒体から転送された著作物を復号する際に、各データブロック固有のデータブロック鍵を生成し、前記機器認証を経て得た固有鍵と、データブロック鍵とを用いて、対応するデータブロックを暗号化して、記録媒体に転送し、若しくは記録媒体から転送されたデータブロックを復号するよいにしてもよい。

### 3. 11 その他の変形例

(1) 上記の実施の形態においては、デジタル著作物保護システムは、メモリカードとメモリメモリカードライタとメモリカードリーダとから構成されるとしているが、デジタル著作物保護システムは、メモリカードとメモリカードライタとから構成されるとしてもよい。また、デジタル著作物保護システムは、メモリカードとメモリカードリーダとから構成されるとしてもよい。

(2) 上記の実施の形態においては、DES暗号を用いるとしているが他の暗号を用いてもよい。

(3) メモリカードは、半導体メモリの代わりに、光ディスク媒体やMO (Magnetoo-Optical) 媒体を有するとしてもよい。

(4) 上記に説明した複数の実施の形態から、いくつかの実施の形態を選んで、組み合わせてもよい。

(5) 本発明は、コンピュータにより実行するプログラムを記録したコンピュータ読み取り可能な記録媒体であって、上記手順をコンピュータに実行させるプログラムを記録していることを特徴とする。

(6) また、前記記録媒体を移送することにより、又は、前記プログラムを通信回線を通して移送することにより、独立した他のコンピュータシステムで実施するようにしてもよい。

【0154】

【発明の効果】

(1)

上記に説明したように、本発明は、記録媒体とアクセス装置とが接続された状態で、両者間で機器認証フェーズと著作物転送フェーズとを実行して著作物の正当者への配布を実現するデジタル著作物保護システムであって、機器認証フェーズでは、記録媒体が所有する固有鍵をアクセス装置に秘密伝送し、アクセス装置が取得した固有鍵を用いて、機器認証を行い、著作物転送フェーズでは、機器認証が成功した場合にのみ、アクセス装置が取得した固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する。

【0155】

この構成によると、適正なアクセス装置が行った認証の手順を模倣する不正な記録装置のリプレイ攻撃に耐えうる強固な認証処理を実現することができるという効果がある。また、不正な装置が適正な装置を欺いて、著作物を不正に読み出し又は著作物を不正に書き込むことを防ぐことができるという効果がある。

(2)

また、本発明は、記録媒体とアクセス装置とが接続された状態で、前記記録媒体と前記アクセス装置との間で機器認証と暗号化された著作物の転送とを行うデジタル著作物保護システムであって、前記記録媒体は、記録媒体毎に異なる固有鍵を予め記憶している固有鍵記憶領域と、接続されたアクセス装置へ前記固有鍵を秘密伝送し、前記固有鍵を用いて前記アクセス装置との間で機器認証を行う第1認証手段と、前記固有鍵を用いて暗号化される著作物を保持するための領域とを備え、前記アクセス装置は、記録媒体から秘密伝送された固有鍵を用いて、前記記録媒体との間で機器認証を行う第2認証手段と、機器認証が成功した場合にのみ、前記機器認証を経て得た固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する転送手段とを備える。

【0156】

この構成によると、適正なアクセス装置が行った認証の手順を模倣する不正な記録装置のリプレイ攻撃に耐えうる強固な認証処理を実現することができるとい

う効果がある。また、不正な装置が適正な装置を欺いて、著作物を不正に読み出し又は著作物を不正に書き込むことを防ぐことができるという効果がある。

(3)

ここで、前記第1認証手段は、あらかじめ第1鍵を有し、前記第1鍵を用いて、前記固有鍵に第1暗号を施して暗号化固有鍵を生成して伝送し、前記第2認証手段は、あらかじめ前記第1鍵を有し、前記第1鍵を用いて、前記伝送された暗号化固有鍵に、前記第1暗号の逆変換を行う第1復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

【0157】

この構成によると、記録装置とアクセス装置とは同一のマスタ鍵を有するので、記録装置とアクセス装置との製造が容易に行えるという効果がある。

(4)

ここで、前記第1認証手段は、第1鍵を基にして、公開鍵暗号方式の公開鍵決定アルゴリズムにより算出された公開鍵である第2鍵をあらかじめ有し、前記第2鍵を用いて、前記固有鍵に第1暗号を施して暗号化固有鍵を生成して伝送し、前記第2認証手段は、あらかじめ前記第1鍵を有し、前記第1鍵を用いて、前記伝送された暗号化固有鍵に、前記第1暗号の逆変換を行う第1復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

【0158】

この構成によると、秘密鍵  $d$  から公開鍵  $e$  を計算できない。なぜならば、秘密鍵  $d$  が分かっているとき、これから  $e$  を求めるためには法  $L$  が知られていなければならないが、 $L$  は  $p-1$  と  $q-1$  の最小公倍数であるため、 $p$  と  $q$  との積を知っているだけでは求められないからである。このことにより、カードリーダー又はカードライターに存在する秘密鍵  $d$  が仮に暴露されたとしてもこれから公開鍵  $e$  を求めることができないので、メモリカードの偽造が困難であるという効果がある。



(5)

ここで、前記第1認証手段は、あらかじめ第1鍵を有し、前記第1鍵を用いて、前記固有鍵に回復型署名処理を施して署名文を生成して伝送し、前記第2認証手段は、前記第1鍵に前記回復型署名処理の公開鍵決定アルゴリズムにより算出された公開鍵である第2鍵をあらかじめ有し、前記第2鍵を用いて、前記伝送された署名文に、前記回復型署名の検証処理を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

【0159】

この構成によると、公開鍵 $K_p$ から秘密鍵 $K_s$ を求めることが、計算量的に非常に困難となる。従って、メモリカードに比べて内部解析の危険性が相対的に高いと思われるメモリライター又はメモリーリーダーに公開鍵を与え、メモリカードに秘密鍵を与える構成が、全体のセキュリティを高めると言う効果がある。

(6)

ここで、前記デジタル著作物保護システムは、さらに固有鍵に第1暗号を施して暗号化固有鍵に変換する固有鍵変換手段を備える暗号化固有鍵作成装置を有し、前記第1認証手段は、前記固有鍵を前記固有鍵変換手段へ出力して変換された暗号化固有鍵を受け取り、受け取った暗号化固有鍵を前記アクセス装置へ伝送し、前記第2認証手段は、記録媒体から伝送された暗号化固有鍵に前記第1暗号の逆処理を行う第1復号を施して固有鍵を生成するように構成してもよい。

【0160】

この構成によると、記録媒体は、変換部を有しないので、回路規模を小さくすることができるという効果を有する。

(7)

ここで、前記第1認証手段は、あらかじめ複数の第1鍵を有し、前記複数の第1鍵のうち一つの第2鍵の選択を受け付け、前記第2鍵を用いて、前記固有鍵に第1暗号を施して暗号化固有鍵を生成して伝送し、前記第2認証手段は、あらかじめ複数の第1鍵を有し、前記複数の第1鍵から前記第2鍵の選択を受け付け、前記第2鍵を用いて、前記伝送された暗号化固有鍵に、前記第1暗号の逆変換を

行う第1復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

【0161】

この構成によると、記録媒体及びアクセス装置は、複数のマスタ鍵を有しているので、複数の異なるデジタル著作物保護システムにおいても適用ができるという効果がある。

(8)

また、本発明は、アクセス装置と接続された状態で、前記アクセス装置との間で機器認証と暗号化された著作物の転送とを行う記録媒体であって、記録媒体毎に異なる固有鍵を記憶している固有鍵記憶領域と、前記固有鍵を用いて暗号化される著作物を保持するための領域と、アクセス装置が接続されたとき、記録媒体から当該アクセス装置へ固有鍵を秘密伝送する手順を経て、当該アクセス装置との間で機器認証を行う認証手段と、機器認証が成功した場合にのみ、前記固有鍵を用いて暗号化された著作物を受け取り前記領域に書き込み若しくは前記領域に記憶されている暗号化された著作物を読み出して前記アクセス装置へ出力する転送手段とを備える。

【0162】

この媒体を用いると、適正なアクセス装置が行った認証の手順を模倣する不正な記録装置のリプレイ攻撃に耐えうる強固な認証処理を実現することができるという効果がある。また、不正な装置が適正な装置を欺いて、著作物を不正に読み出し又は著作物を不正に書き込むことを防ぐことができるという効果がある。

(9)

また、本発明は、固有鍵を有する記録媒体と接続され、前記記録媒体との間で機器認証と暗号化された著作物の転送とを行うアクセス装置であって、記録媒体から固有鍵を秘密伝送される手順を経て、前記記録媒体との間で機器認証を行う認証手段と、機器認証が成功した場合にのみ、前記機器認証を経て得た固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する転送手段とを備える。

## 【0163】

このアクセス装置を用いると、適正なアクセス装置が行った認証の手順を模倣する不正な記録装置のリプレイ攻撃に耐えうる強固な認証処理を実現することができるという効果がある。また、不正な装置が適正な装置を欺いて、著作物を不正に読み出し又は著作物を不正に書き込むことを防ぐことができるという効果がある。

## (10)

また、本発明は、記録媒体とアクセス装置とが接続された状態で、両者間で機器認証ステップと著作物転送ステップとを実行して著作物の正当者への配布を実現するデジタル著作物保護方法であって、機器認証ステップでは、記録媒体が所有する固有鍵をアクセス装置に秘密伝送し、アクセス装置が取得した固有鍵を用いて、機器認証を行い、著作物転送ステップでは、機器認証が成功した場合にのみ、アクセス装置が取得した固有鍵を用いて著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号する。

## 【0164】

この方法を用いると、適正なアクセス装置が行った認証の手順を模倣する不正な記録装置のリプレイ攻撃に耐えうる強固な認証処理を実現することができるという効果がある。また、不正な装置が適正な装置を欺いて、著作物を不正に読み出し又は著作物を不正に書き込むことを防ぐことができるという効果がある。

## (11)

また、本発明は、記録媒体毎に異なる固有鍵を予め記憶している固有鍵記憶領域及び前記固有鍵を用いて暗号化される著作物を保持するための領域を有する記録媒体とアクセス装置とが接続された状態で、前記記録媒体と前記アクセス装置との間で機器認証と暗号化された著作物の転送とを行うデジタル著作物保護システムで用いられるデジタル著作物保護方法であって、接続されたアクセス装置へ前記固有鍵を秘密伝送し、前記固有鍵を用いて前記アクセス装置との間で機器認証を行う第1認証ステップと、記録媒体から秘密伝送された固有鍵を用いて、前記記録媒体との間で機器認証を行う第2認証ステップと、機器認証が成功した場合にのみ、前記機器認証を経て得た固有鍵を用いて著作物を暗号化して記録媒体

に転送し若しくは記録媒体から転送された著作物を復号する転送ステップとを含む。

【0165】

この方法を用いると、適正なアクセス装置が行った認証の手順を模倣する不正な記録装置のリプレイ攻撃に耐えうる強固な認証処理を実現することができるという効果がある。また、不正な装置が適正な装置を欺いて、著作物を不正に読み出し又は著作物を不正に書き込むことを防ぐことができるという効果がある。

(12)

ここで、前記第1認証ステップは、あらかじめ第1鍵を有し、前記第1鍵を用いて、前記固有鍵に第1暗号を施して暗号化固有鍵を生成して伝送し、前記第2認証ステップは、あらかじめ前記第1鍵を有し、前記第1鍵を用いて、前記伝送された暗号化固有鍵に、前記第1暗号の逆変換を行う第1復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送ステップは、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

【0166】

この方法を用いると、記録装置とアクセス装置とは同一のマスタ鍵を有するので、記録装置とアクセス装置との製造が容易に行えるという効果がある。

(13)

ここで、前記第1認証ステップは、第1鍵を基にして、公開鍵暗号方式の公開鍵決定アルゴリズムにより算出された公開鍵である第2鍵をあらかじめ有し、前記第2鍵を用いて、前記固有鍵に第1暗号を施して暗号化固有鍵を生成して伝送し、前記第2認証ステップは、あらかじめ前記第1鍵を有し、前記第1鍵を用いて、前記伝送された暗号化固有鍵に、前記第1暗号の逆変換を行う第1復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送ステップは、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

【0167】

この方法を用いると、秘密鍵  $d$  から公開鍵  $e$  を計算できない。なぜならば、秘

密鍵  $d$  が分かっているとき、これから  $e$  を求めるためには法  $L$  が知られていなければならないが、 $L$  は  $p-1$  と  $q-1$  の最小公倍数であるため、 $p$  と  $q$  との積を知っているだけでは求められないからである。このことにより、カードリーダー又はカードライターに存在する秘密鍵  $d$  が仮に暴露されたとしてもこれから公開鍵  $e$  を求めることができないので、メモリカードの偽造が困難であるという効果がある。

(14)

ここで、前記第1認証ステップは、あらかじめ第1鍵を有し、前記第1鍵を用いて、前記固有鍵に回復型署名処理を施して署名文を生成して伝送し、前記第2認証ステップは、前記第1鍵に前記回復型署名処理の公開鍵決定アルゴリズムにより算出された公開鍵である第2鍵をあらかじめ有し、前記第2鍵を用いて、前記伝送された署名文に、前記回復型署名の検証処理を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送ステップは、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

【0168】

この方法を用いると、公開鍵  $K_p$  から秘密鍵  $K_s$  を求めることが、計算量的に非常に困難となる。従って、メモリカードに比べて内部解析の危険性が相対的に高いと思われるメモリライター又はメモリリーダーに公開鍵を与え、メモリカードに秘密鍵を与える構成が、全体のセキュリティを高めると言う効果がある。

(15)

ここで、前記デジタル著作物保護システムは、さらに固有鍵に第1暗号を施して暗号化固有鍵に変換する固有鍵変換手段を備える暗号化固有鍵作成装置を有し、前記第1認証ステップは、前記固有鍵を前記固有鍵変換手段へ出力して変換された暗号化固有鍵を受け取り、受け取った暗号化固有鍵を前記アクセス装置へ伝送し、前記第2認証ステップは、記録媒体から伝送された暗号化固有鍵に前記第1暗号の逆処理を行う第1復号を施して固有鍵を生成するように構成してもよい。

【0169】

この方法を用いると、記録媒体は、変換部を有しないので、回路規模を小さく

することができるという効果を有する。

(16)

ここで、前記第1認証ステップは、あらかじめ複数の第1鍵を有し、前記複数の第1鍵のうち一つの第2鍵の選択を受け付け、前記第2鍵を用いて、前記固有鍵に第1暗号を施して暗号化固有鍵を生成して伝送し、前記第2認証ステップは、あらかじめ複数の第1鍵を有し、前記複数の第1鍵から前記第2鍵の選択を受け付け、前記第2鍵を用いて、前記伝送された暗号化固有鍵に、前記第1暗号の逆変換を行う第1復号を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送ステップは、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

【0170】

この方法を用いると、記録媒体及びアクセス装置は、複数のマスタ鍵を有しているので、複数の異なるデジタル著作物保護システムにおいても適用ができるという効果がある。

(17)

また、本発明は、以上に説明したデジタル著作物保護方法をコンピュータに実行させるプログラムを記録したコンピュータ読み取り可能な記録媒体であり、前記プログラムにより上記方法をコンピュータに実行させることにより、上記デジタル著作物保護システムと同様の効果を奏することは明らかである。

(18)

ここで、前記第1認証手段は、第3鍵を用いて前記固有鍵に第1変換を施して変形鍵を生成し、前記第1鍵を用いて、前記変形鍵に第2変換を施して、暗号化固有鍵を生成して伝送し、前記第2認証手段は、前記第1鍵を用いて、前記伝送された暗号化固有鍵に、前記第2変換の逆変換を行う第2逆変換を施して、復号変形鍵を生成し、前記第3鍵を用いて、前記復号変形鍵に、前記第1変換の逆変換を行う第1逆変換を施して、復号固有鍵を生成し、前記復号固有鍵を用いて、前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

【0171】

この構成によると、1つのデジタル著作物運用システムを複数の団体が運営する場合、これらの団体の数だけ、異なるサブグループ鍵が存在し、これらの異なるサブグループ鍵が、それぞれ前記複数の団体に割り当てられるので、各団体は、独自のサービスの提供が可能となる。また、また、メモ리카ードの記憶容量は限られているので、メモ리카ードに記憶できるマスタ鍵の数には制限がある場合が多く、マスタ鍵とサブグループ鍵との組合せにより用いることができる鍵の数を増やすことができるという効果がある。

(19)

ここで、前記第1認証手段は、第1鍵を用いて前記固有鍵に第2変換を施して変形鍵を生成し、前記第3鍵を用いて、前記変形鍵に第1変換を施して暗号化固有鍵を生成して伝送し、前記第2認証手段は、前記第3鍵を用いて、前記伝送された暗号化固有鍵に、前記第1変換の逆変換を行う第1逆変換を施して、復号変形鍵を生成し、前記第1鍵を用いて、前記復号変形鍵に、前記第2変換の逆変換を行う第2逆変換を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

【0172】

この構成によると、1つのデジタル著作物運用システムを複数の団体が運営する場合、これらの団体の数だけ、異なるサブグループ鍵が存在し、これらの異なるサブグループ鍵が、それぞれ前記複数の団体に割り当てられるので、各団体は、独自のサービスの提供が可能となる。また、また、メモ리카ードの記憶容量は限られているので、メモ리카ードに記憶できるマスタ鍵の数には制限がある場合が多く、マスタ鍵とサブグループ鍵との組合せにより用いることができる鍵の数を増やすことができるという効果がある。

(20)

ここで、前記第1認証手段は、前記第3鍵を用いて、第1鍵に第1変換を施して、変形第1鍵を生成し、前記変形第1鍵を用いて、前記固有鍵に第2変換を施して暗号化固有鍵を生成して伝送し、前記第2認証手段は、前記第3鍵を用いて、第1鍵に第1変換を施して、変形第1鍵を生成し、前記変形第1鍵を用いて、

前記伝送された暗号化固有鍵に、前記第2変換の逆変換を行う第2逆変換を施して、復号固有鍵を生成し、前記復号固有鍵を用いて前記記録媒体との間で機器認証を行い、前記転送手段は、前記復号固有鍵を用いて著作物の転送を行うように構成してもよい。

### 【0173】

この構成によると、1つのデジタル著作物運用システムを複数の団体が運営する場合、これらの団体の数だけ、異なるサブグループ鍵が存在し、これらの異なるサブグループ鍵が、それぞれ前記複数の団体に割り当てられるので、各団体は、独自のサービスの提供が可能となる。また、また、メモ리카ードの記憶容量は限られているので、メモ리카ードに記憶できるマスタ鍵の数には制限がある場合が多く、マスタ鍵とサブグループ鍵との組合せにより用いることができる鍵の数を増やすことができるという効果がある。

### (21)

ここで、前記第1認証手段は、前記第1鍵を用いて、前記固有鍵に第2変換を施して、暗号化固有鍵を生成して伝送し、前記固有鍵に第3鍵を用いて第1変換を施して変形固有鍵を生成し、前記第2認証手段は、前記第1鍵を用いて、前記伝送された暗号化固有鍵に、前記第1鍵を用いて、前記第2変換の逆変換を行う第2逆変換を施して、復号固有鍵を生成し、前記固有鍵に第3鍵を用いて、第1変換を施して、変形復号固有鍵を生成し、前記変形復号固有鍵を用いて、前記記録媒体との間で機器認証を行い、前記転送手段は、前記変形復号固有鍵を用いて著作物の転送を行うように構成してもよい。

### 【0174】

この構成によると、1つのデジタル著作物運用システムを複数の団体が運営する場合、これらの団体の数だけ、異なるサブグループ鍵が存在し、これらの異なるサブグループ鍵が、それぞれ前記複数の団体に割り当てられるので、各団体は、独自のサービスの提供が可能となる。また、また、メモ리카ードの記憶容量は限られているので、メモ리카ードに記憶できるマスタ鍵の数には制限がある場合が多く、マスタ鍵とサブグループ鍵との組合せにより用いることができる鍵の数を増やすことができるという効果がある。



(22)

ここで、前記著作物が、ある論理的若しくは物理的単位毎に1つ以上のデータブロックにより構成されているものとし、前記著作物の各データブロックを暗号化して記録媒体に転送し、若しくは記録媒体から転送された著作物を復号する際に、前記転送手段は、各データブロック固有のデータブロック鍵を生成し、前記機器認証を経て得た固有鍵と、データブロック鍵とを用いて、対応するデータブロックを暗号化して、記録媒体に転送し、若しくは記録媒体から転送されたデータブロックを復号するように構成してもよい。

【0175】

この構成によると、著作物を形成するデータブロック毎に、異なるデータブロック鍵を生成し、生成された異なるデータブロック鍵でデータブロック単位の著作物を暗号化するので、データブロックが盗聴されにくくなり、データブロックの安全性が向上するという効果がある。

(23)

ここで、前記著作物が、1つ以上のファイルに構成されているものとし、前記著作物の各ファイルを暗号化して記録媒体に転送し、若しくは記録媒体から転送された著作物を復号する際に、前記転送手段は、各ファイル固有のファイル鍵を生成し、前記機器認証を経て得た固有鍵と、ファイル鍵を用いて、対応するファイルを暗号化して記録媒体に転送し、若しくは記録媒体から転送されたファイルを復号するように構成してもよい。

【0176】

この構成によると、著作物を形成するファイル毎に、異なるファイル鍵を生成し、生成された異なるファイル鍵でファイル単位の著作物を暗号化するので、ファイルが盗聴されにくくなり、ファイルの安全性が向上するという効果がある。

(24)

ここで、前記アクセス装置は、さらに、操作者からユーザ鍵の入力を受け付けるユーザ鍵受付手段と、前記入力を受け付けられたユーザ鍵と、記憶媒体から秘密伝送された固有鍵とを基にして、変形鍵を生成する変形鍵生成手段とを有し、前記転送手段は、機器認証が成功した場合にのみ、前記生成された変形鍵を用い

て著作物を暗号化して記録媒体に転送し若しくは記録媒体から転送された著作物を復号するように構成してもよい。

【0177】

この構成によると、ユーザは、自分で設定したユーザ鍵を用いて著作物を暗号化し、暗号化した著作物を前記ユーザ鍵を用いて復号できるので、ユーザ自身の著作物が他人に解読されず、保護できるという効果がある。

【図面の簡単な説明】

【図1】

本発明に係る一つの実施の形態としてのデジタル著作物保護システム100のブロック図を示す。

【図2】

メモリカード200がメモリカードライタ300に装着され、メモリカードライタ300がパーソナルコンピュータ500に装着される状態を示す。

【図3】

メモリカード200がメモリカードリーダー400の一種であるヘッドホンステレオ401に装着される状態を示す。

【図4】

メモリカード200の構成を示すブロック図である。

【図5】

メモリカードライタ300の構成を示すブロック図である。

【図6】

メモリカードリーダー400の構成を示すブロック図である。

【図7】

メモリカード200が、メモリカードライタ300に装着された場合の概要動作を示すフローチャートである。

【図8】

メモリカード200が、メモリカードリーダー400に装着された場合の概要動作を示すフローチャートである。

【図9】

メモリカード 200 が、メモリカードライター 300 に装着された場合の詳細の認証動作を示す。

【図 10】

メモリカード 200 が、メモリカードライター 300 に装着された場合の詳細の認証動作を示す。

【図 11】

本発明に係るまた別の実施の形態の一つとしてのデジタル著作物保護システム 100 a の構成を示すブロック図である。

【図 12】

メモリカード 200 a が、メモリカードライター 300 に装着された場合の詳細の認証動作を示す。

【図 13】

本発明に係るまた別の実施の形態の一つとしてのデジタル著作物保護システムにおいて、メモリカード 200 がメモリカードライター 300 に装着された場合の詳細の認証動作を示す。

【図 14】

本発明に係るまた別の実施の形態の一つとしてのデジタル著作物保護システム 100 c におけるメモリカード 200 c の構成を示すブロック図である。

【図 15】

デジタル著作物保護システム 100 c におけるメモリカードライター 300 c の構成を示すブロック図である。

【図 16】

デジタル著作物保護システム 100 c におけるメモリカードリーダー 400 c の構成を示すブロック図である。

【図 17】

デジタル著作物保護システム 100 d の構成を示すブロック図である。

【図 18】

デジタル著作物保護システム 100 d の動作を示す。

【図 19】

デジタル著作物保護システム 100e の構成を示すブロック図である。

【図 20】

デジタル著作物保護システム 100e の動作を示す。

【図 21】

デジタル著作物保護システム 100f の構成を示すブロック図である。

【図 22】

デジタル著作物保護システム 100f の動作を示す。

【図 23】

デジタル著作物保護システム 100g の構成を示すブロック図である。

【図 24】

デジタル著作物保護システム 100g の動作を示す。

【図 25】

デジタル著作物保護システム 100h の構成を示すブロック図である。

【図 26】

デジタル著作物保護システム 100h の構成を示すブロック図である。

【図 27】

デジタル著作物保護システム 100h の動作を示すブロック図である。

【図 28】

デジタル著作物保護システム 100h の動作を示すブロック図である。

【図 29】

デジタル著作物保護システム 100i の構成を示すブロック図である。

【図 30】

デジタル著作物保護システム 100i の構成を示すブロック図である。

【図 31】

デジタル著作物保護システム 100i の動作を示すブロック図である。

【図 32】

デジタル著作物保護システム 100i の動作を示すブロック図である。

【図 33】

デジタル著作物保護システム 100i の別の構成を示すブロック図である。

【図 34】

デジタル著作物保護システム 100 i の別の構成を示すブロック図である。

【符号の説明】

- 10 通信回線
- 100、100 a、100 c、100 d、100 e、100 f、100 g、  
100 h、100 i デジタル著作物保護システム
- 200 メモリカード
- 210 マスタ鍵記憶部
- 220 メディア固有鍵記憶部
- 221 装置鍵記憶部
- 222 逆変換部
- 223 装置鍵情報記憶部
- 230 変換部
- 240 メディア固有鍵情報記憶部
- 250 相互認証部
- 251 乱数発生部
- 252 暗号部
- 253 復号部
- 254 相互認証制御部 254
- 260 暗号化著作物記憶部
- 270 通信部
- 280 制御部
- 300 メモリカードライタ
- 310 装置鍵記憶部
- 311 変換部
- 312 装置鍵情報記憶部
- 313 マスタ鍵記憶部
- 320 メディア固有鍵情報記憶部
- 321 逆変換部

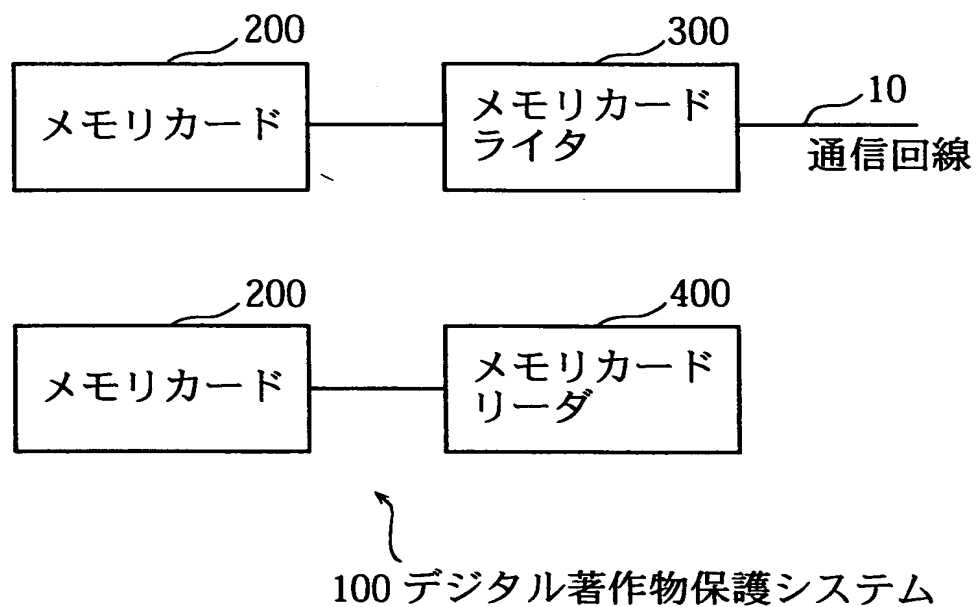
323 メディア固有鍵記憶部  
330 相互認証部  
331 乱数発生部  
332 暗号部  
333 復号部  
334 相互認証制御部  
340 通信部  
350 制御部  
360 暗号部  
370 著作物記憶部  
380 著作物取得部  
400 メモリカードリーダー  
410 装置鍵記憶部  
411 変換部  
412 装置鍵情報記憶部  
413 マスタ鍵記憶部  
420 メディア固有鍵情報記憶部  
421 逆変換部  
423 メディア固有鍵記憶部  
430 相互認証部  
431 乱数発生部  
432 暗号部  
433 復号部  
434 相互認証制御部  
440 通信部  
450 制御部  
460 復号部  
470 著作物記憶部  
480 再生部

特平 1 0 — 3 3 9 0 2 7

4 9 0 操作部

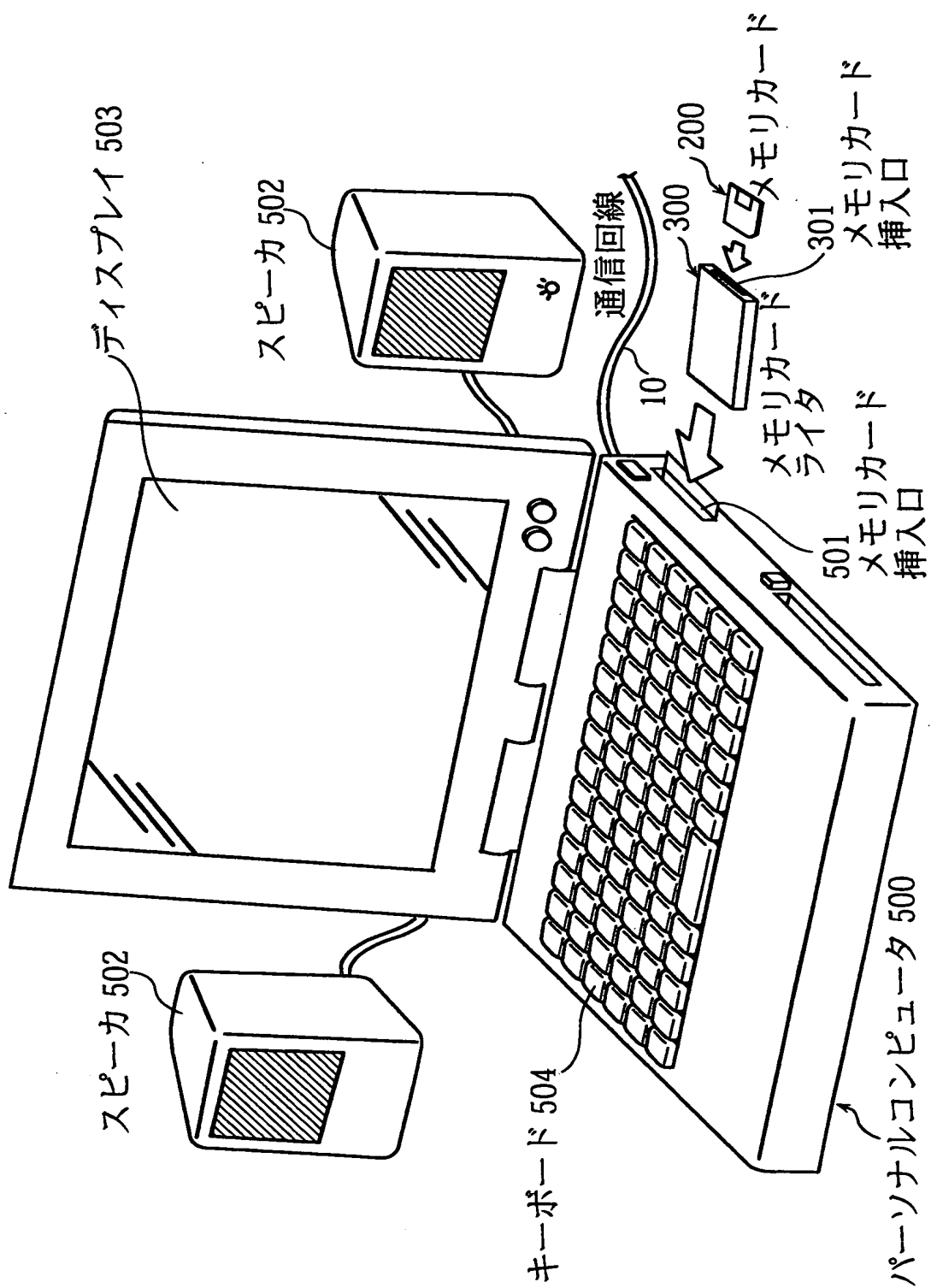
【書類名】 図面

【図 1】

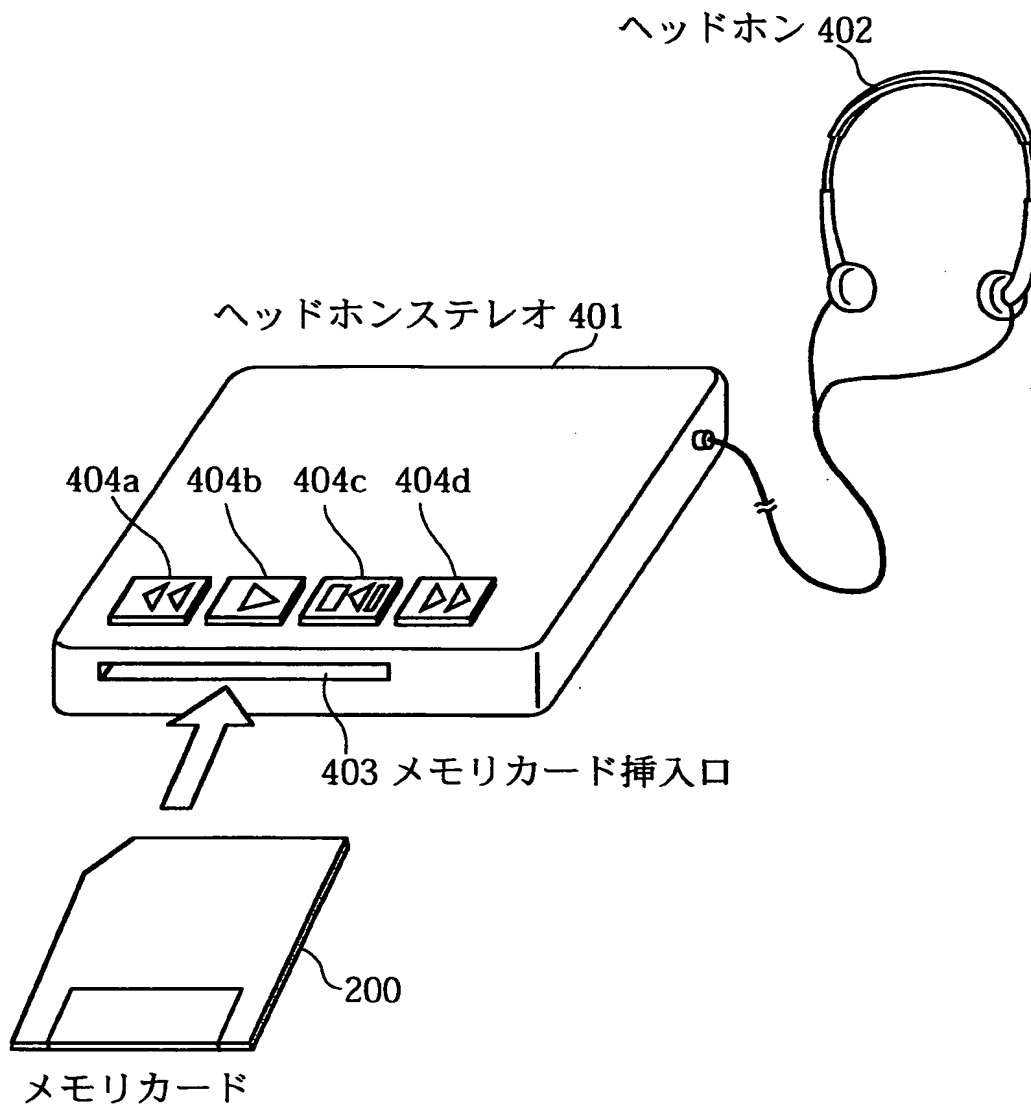




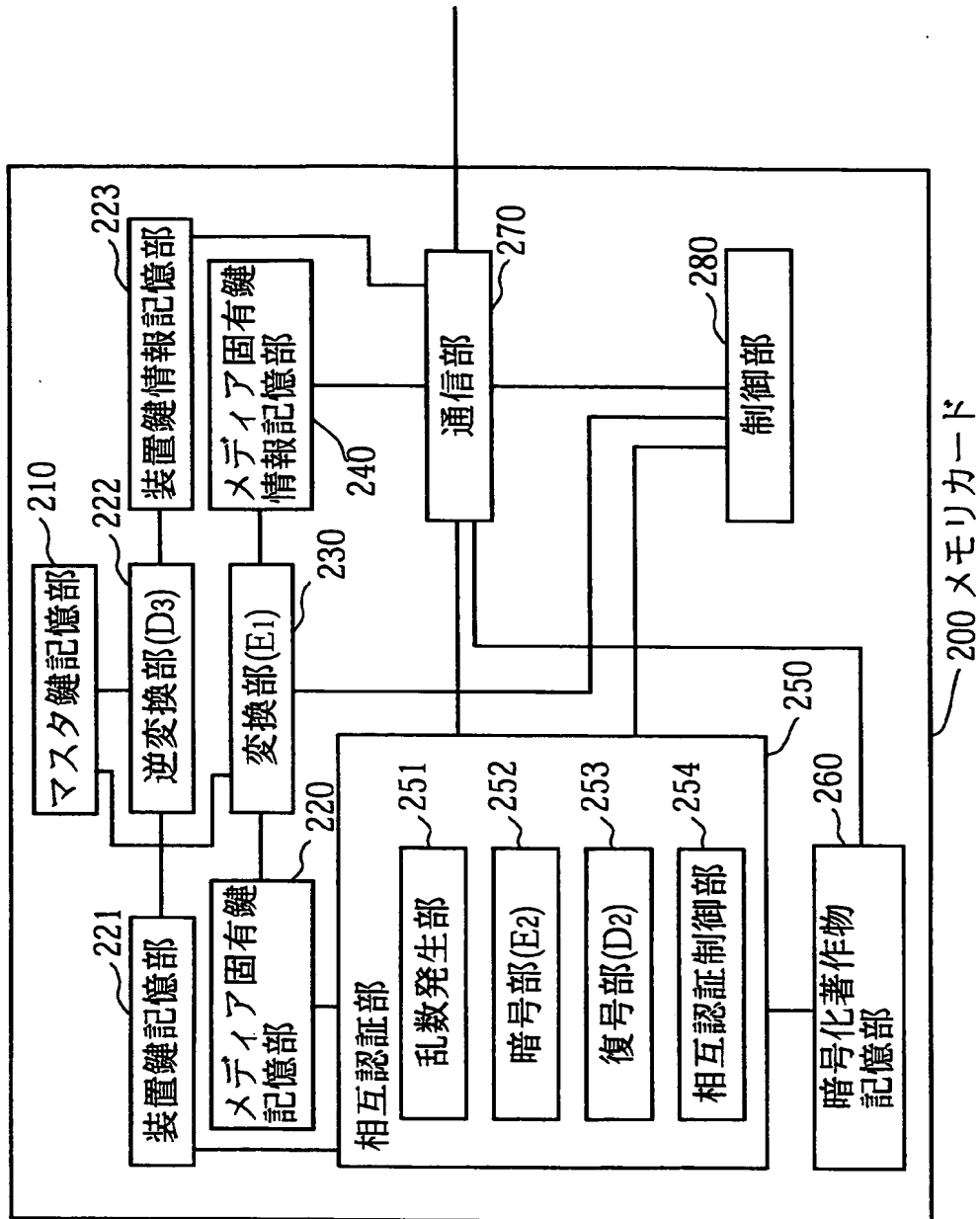
【図 2】



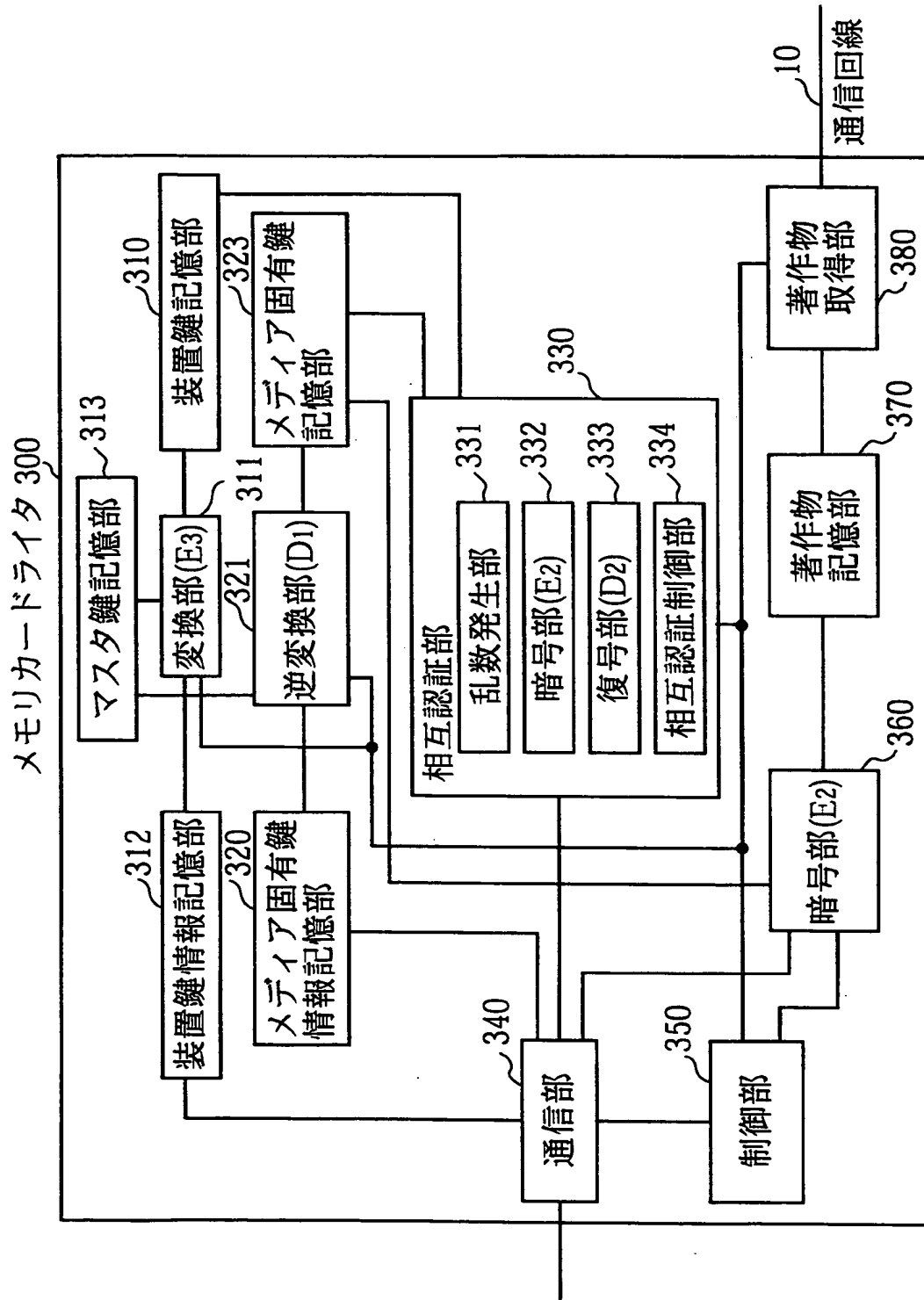
【図 3】



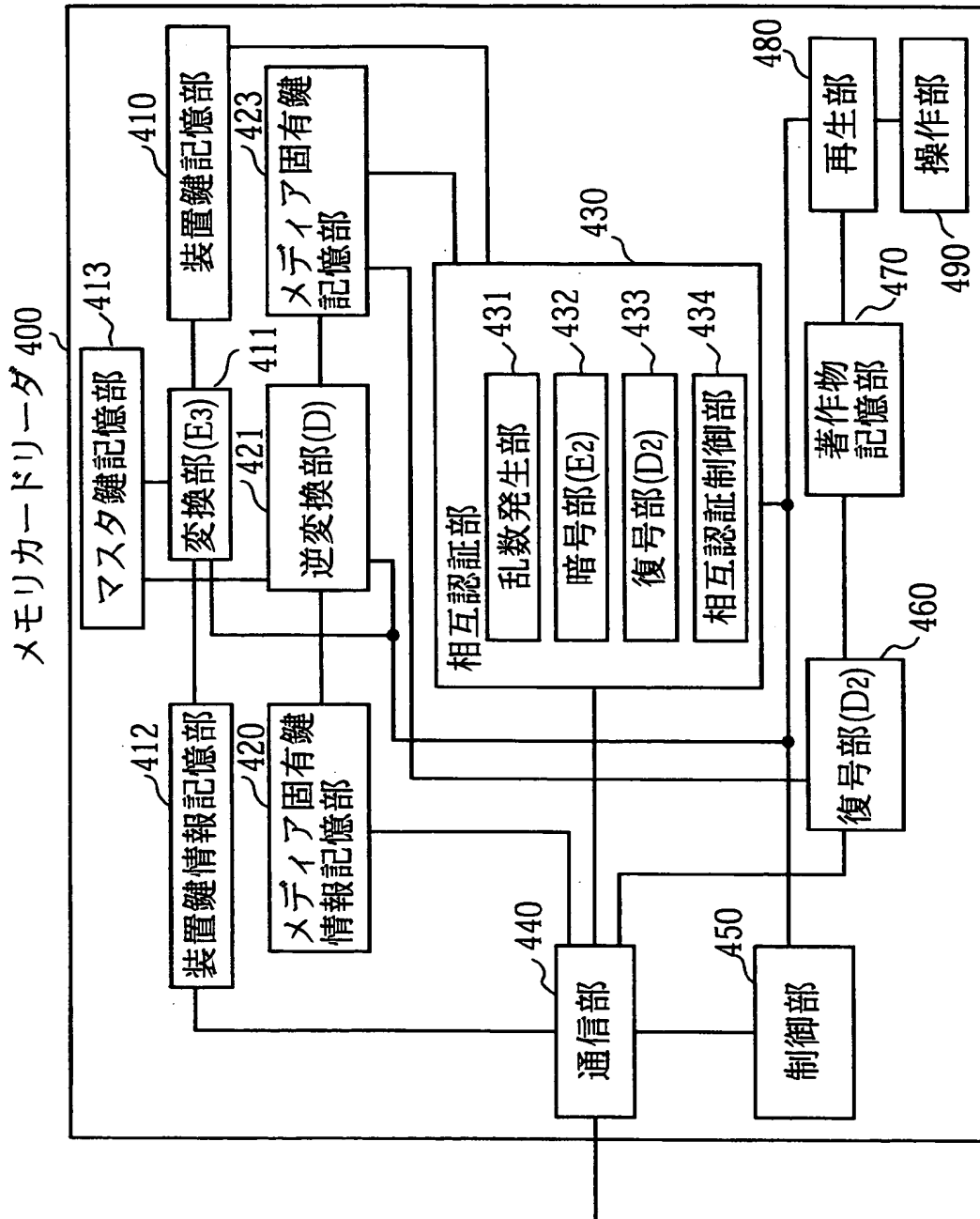
【図 4】



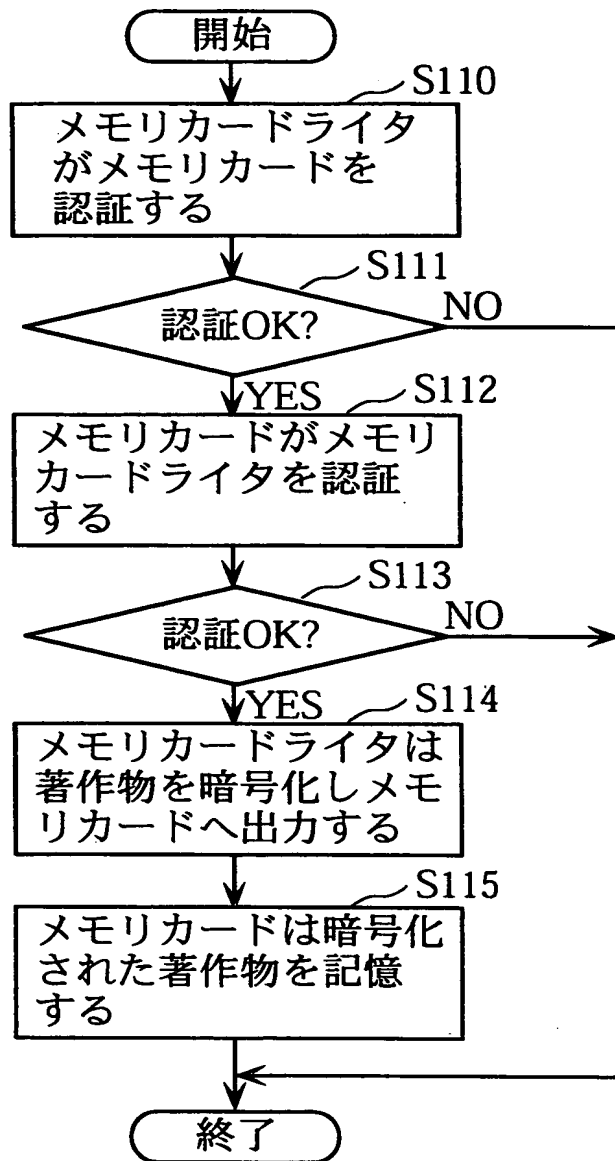
【図 5】



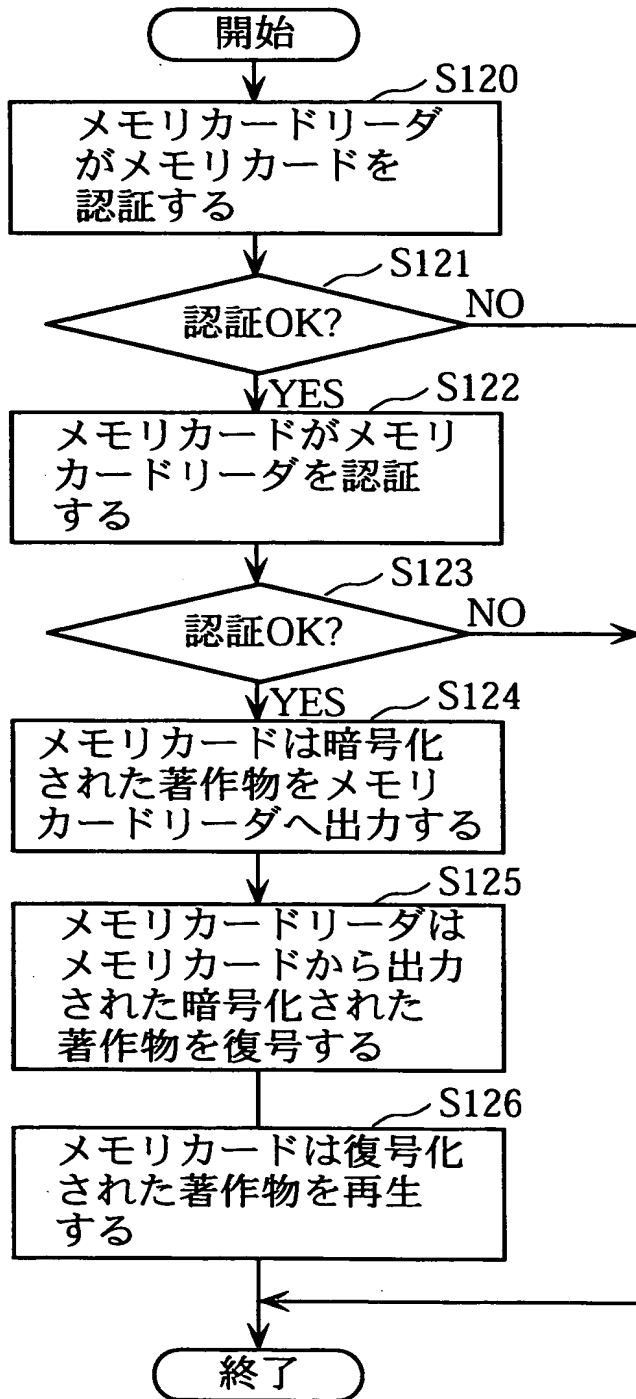
【図 6】



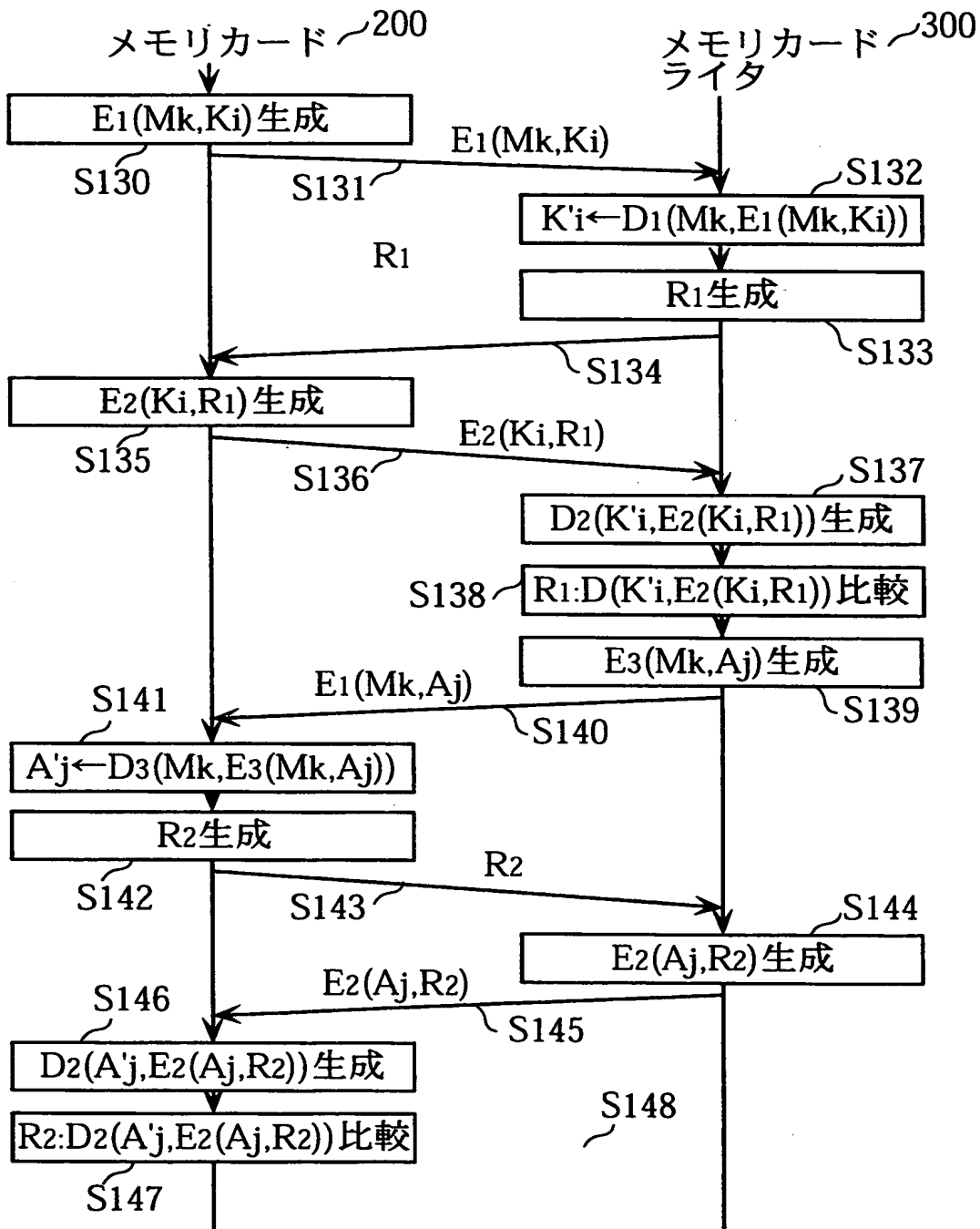
【図 7】



【図 8】

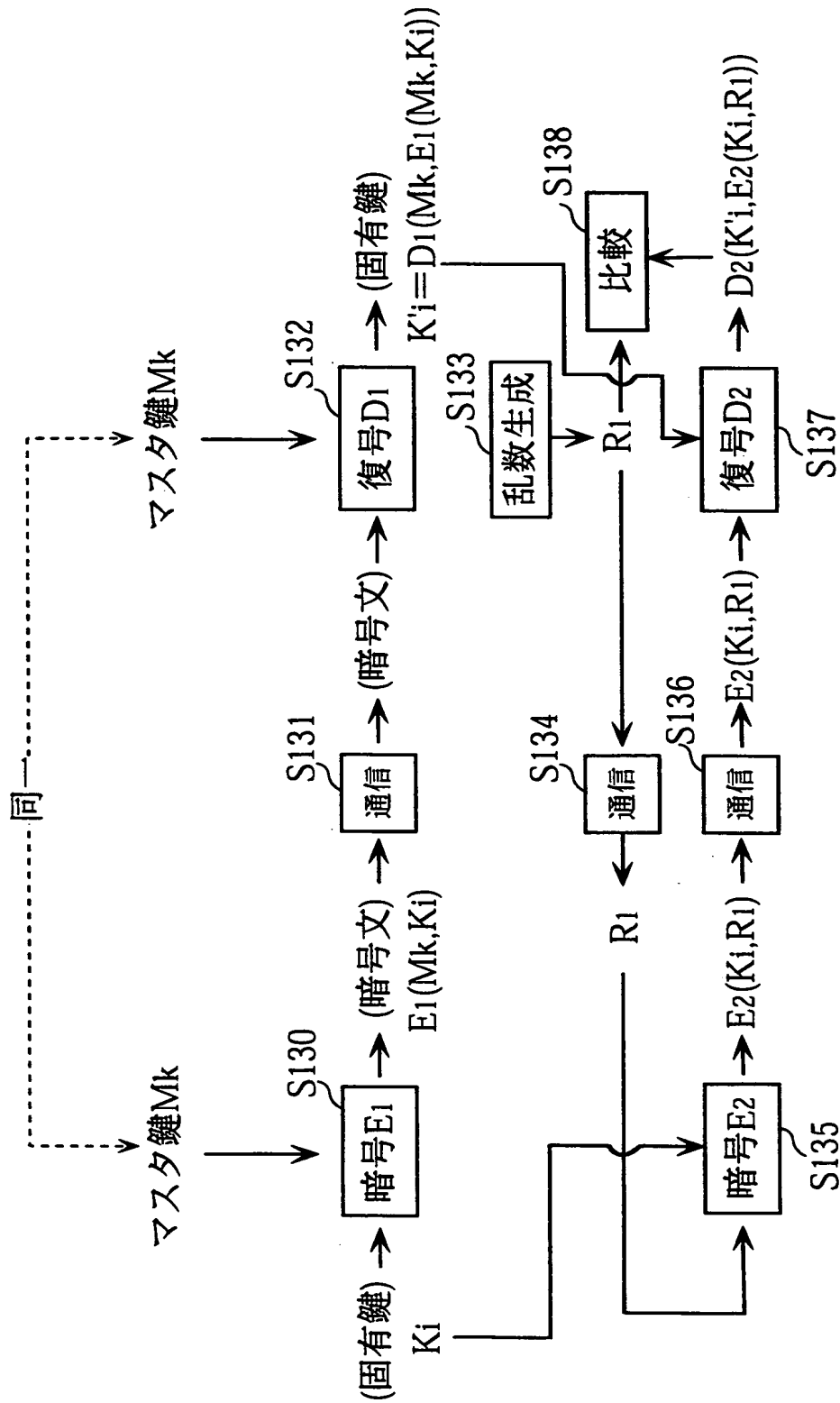


【図9】

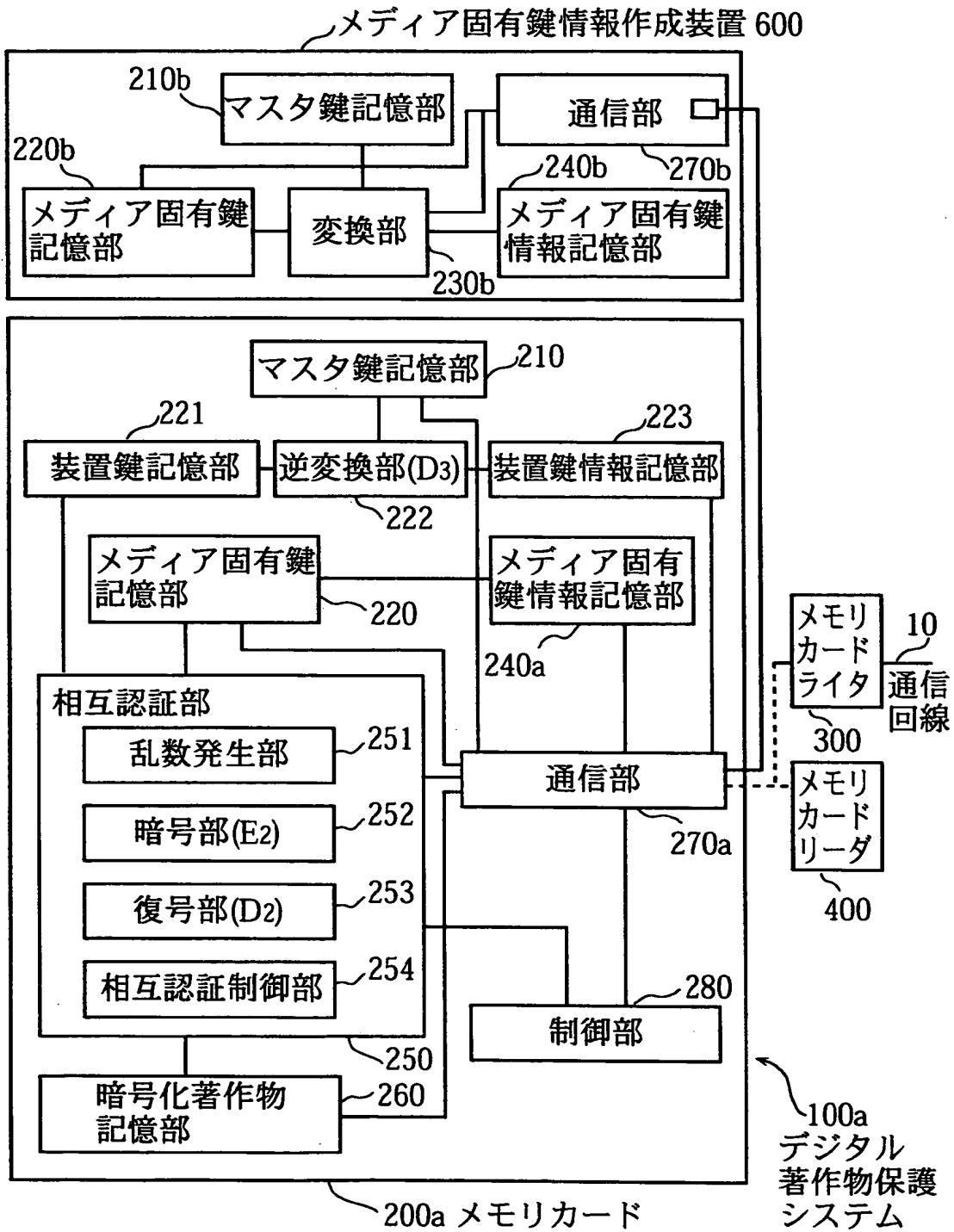




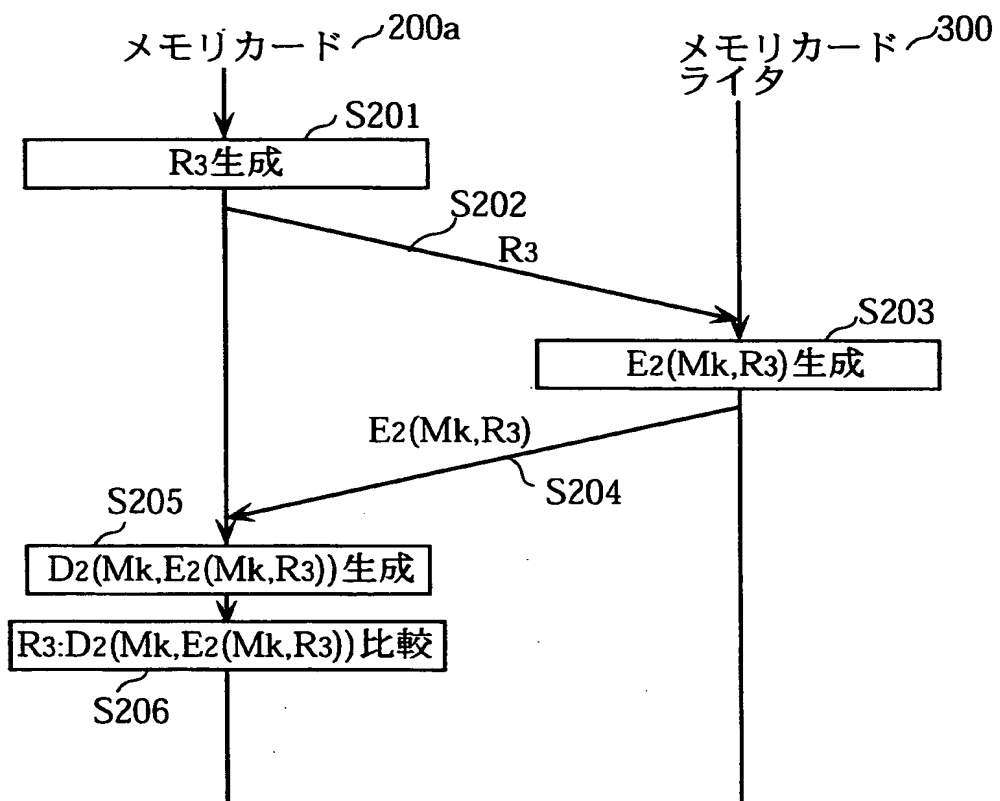
【図 10】



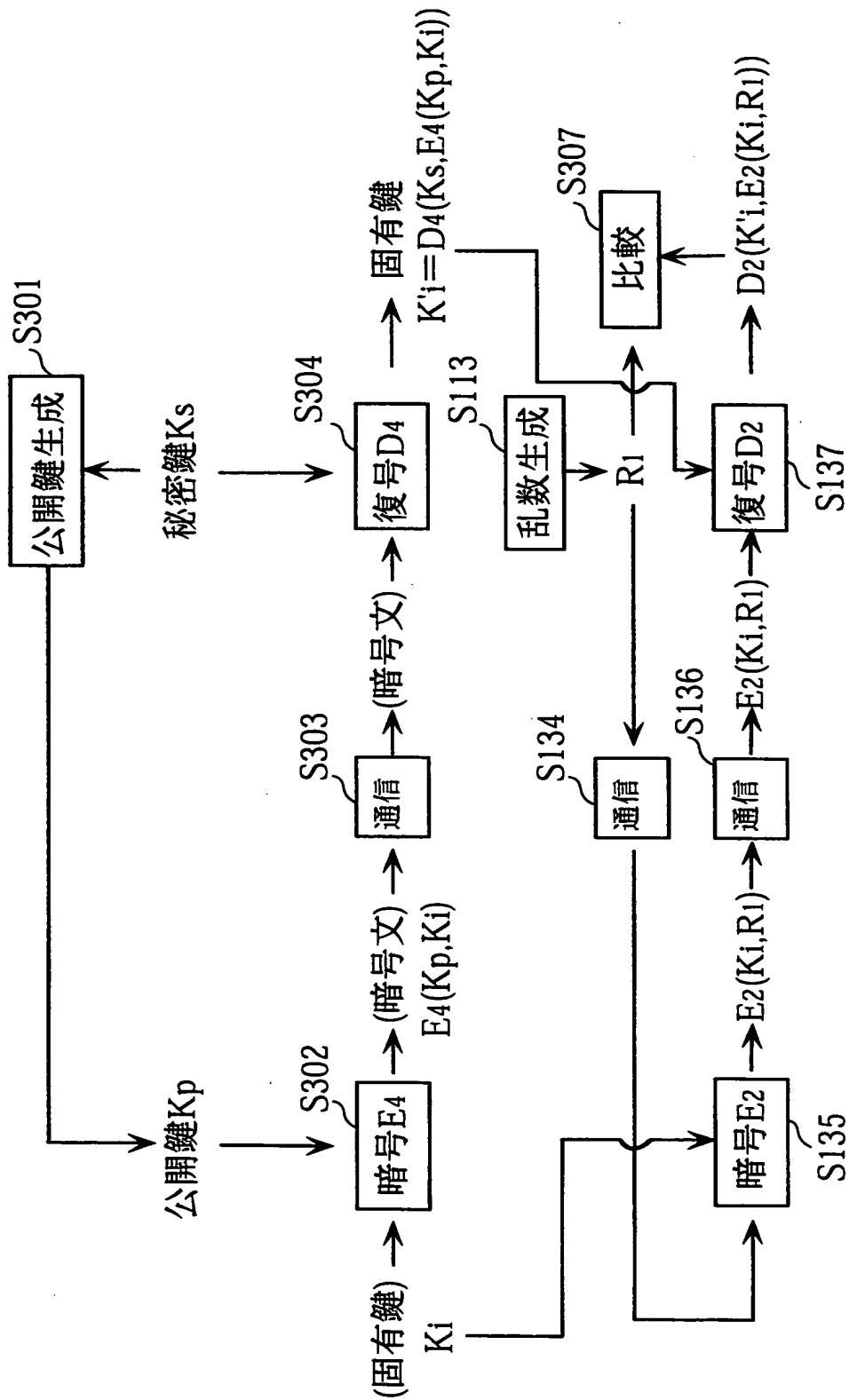
【図 11】



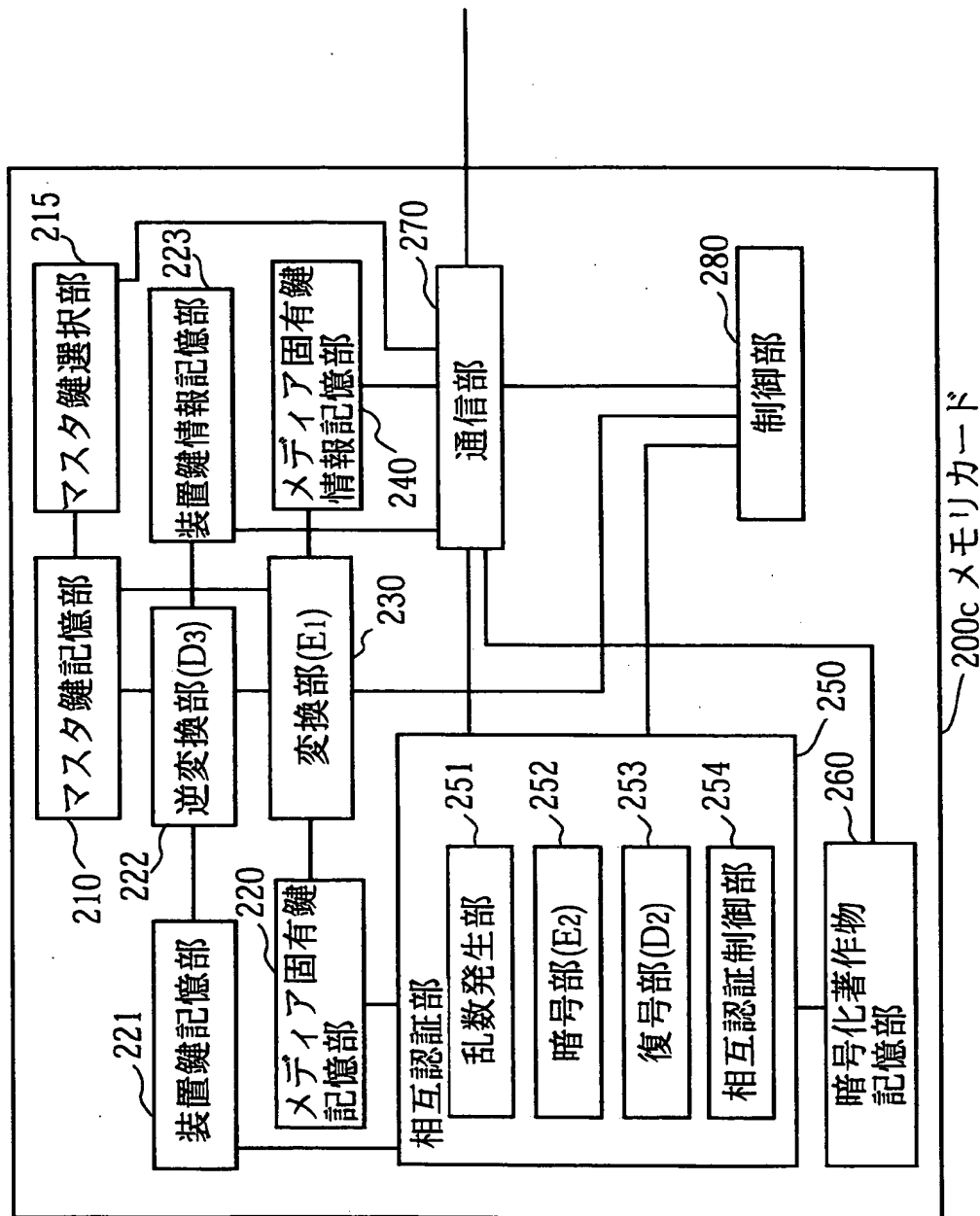
【図 12】



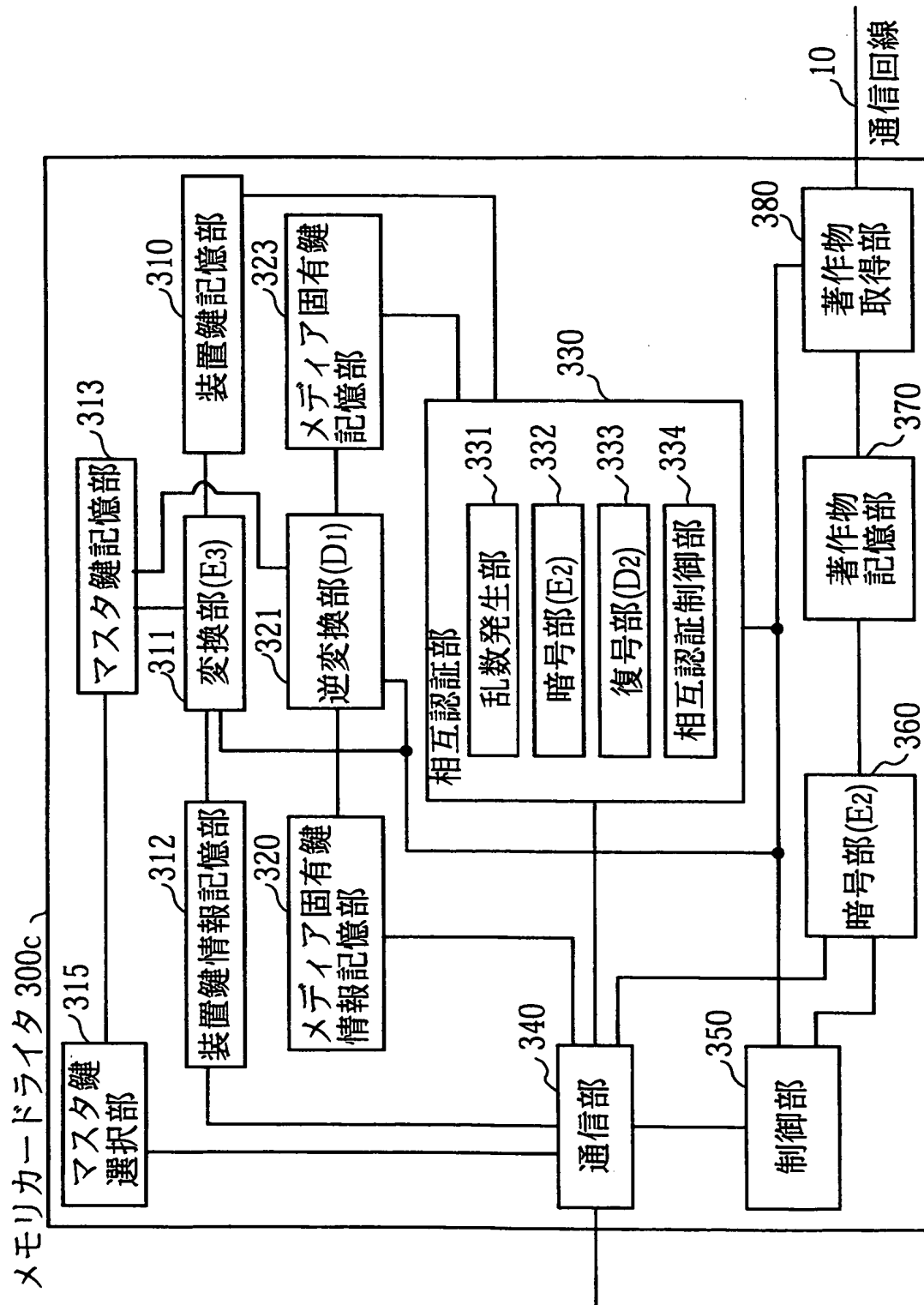
【図 13】



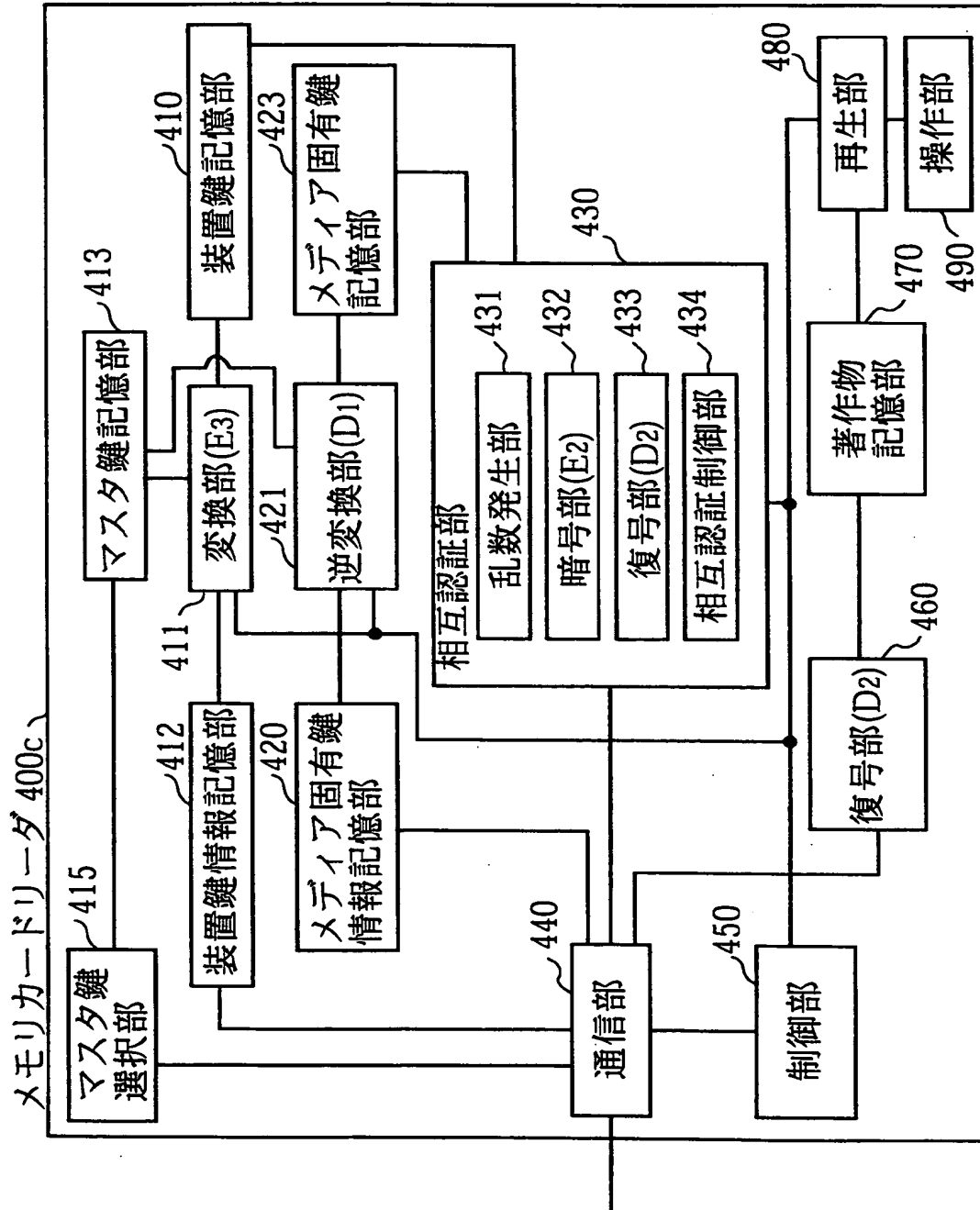
【図 14】



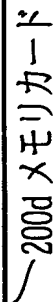
【図 1 5】



【図 16】

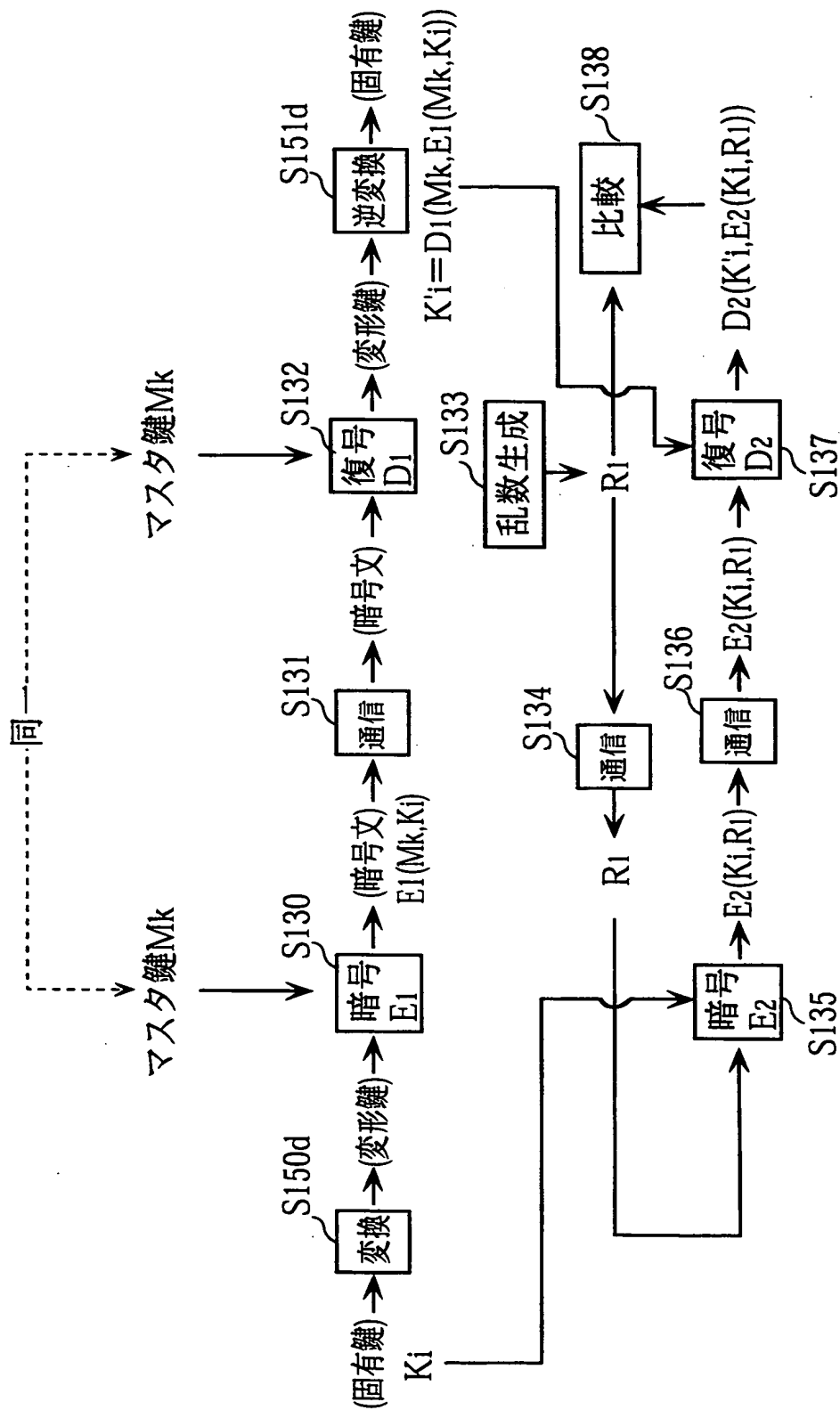


デジタル著作物  
保護システム 100d  
メモ리카ードライタ 300d

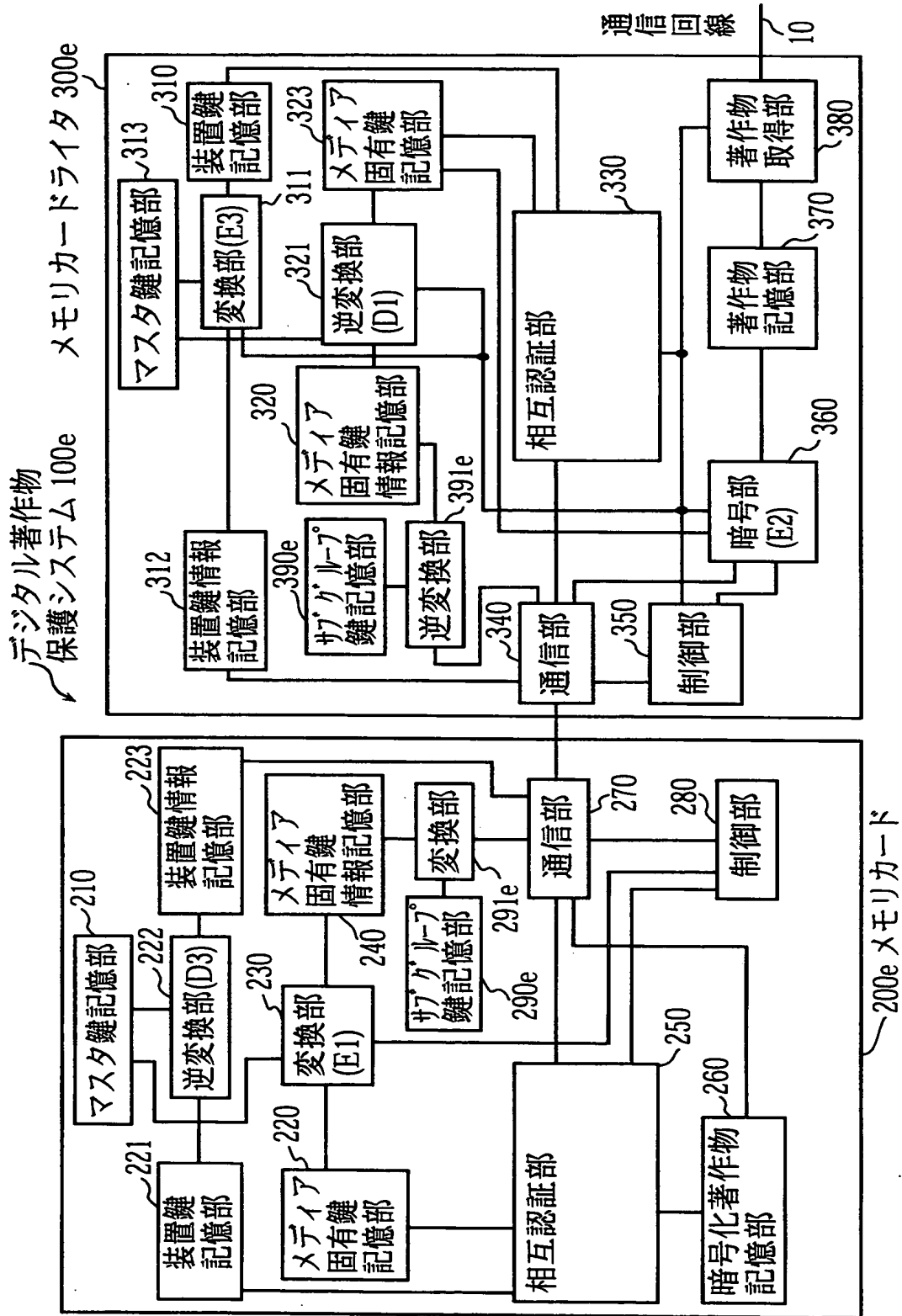




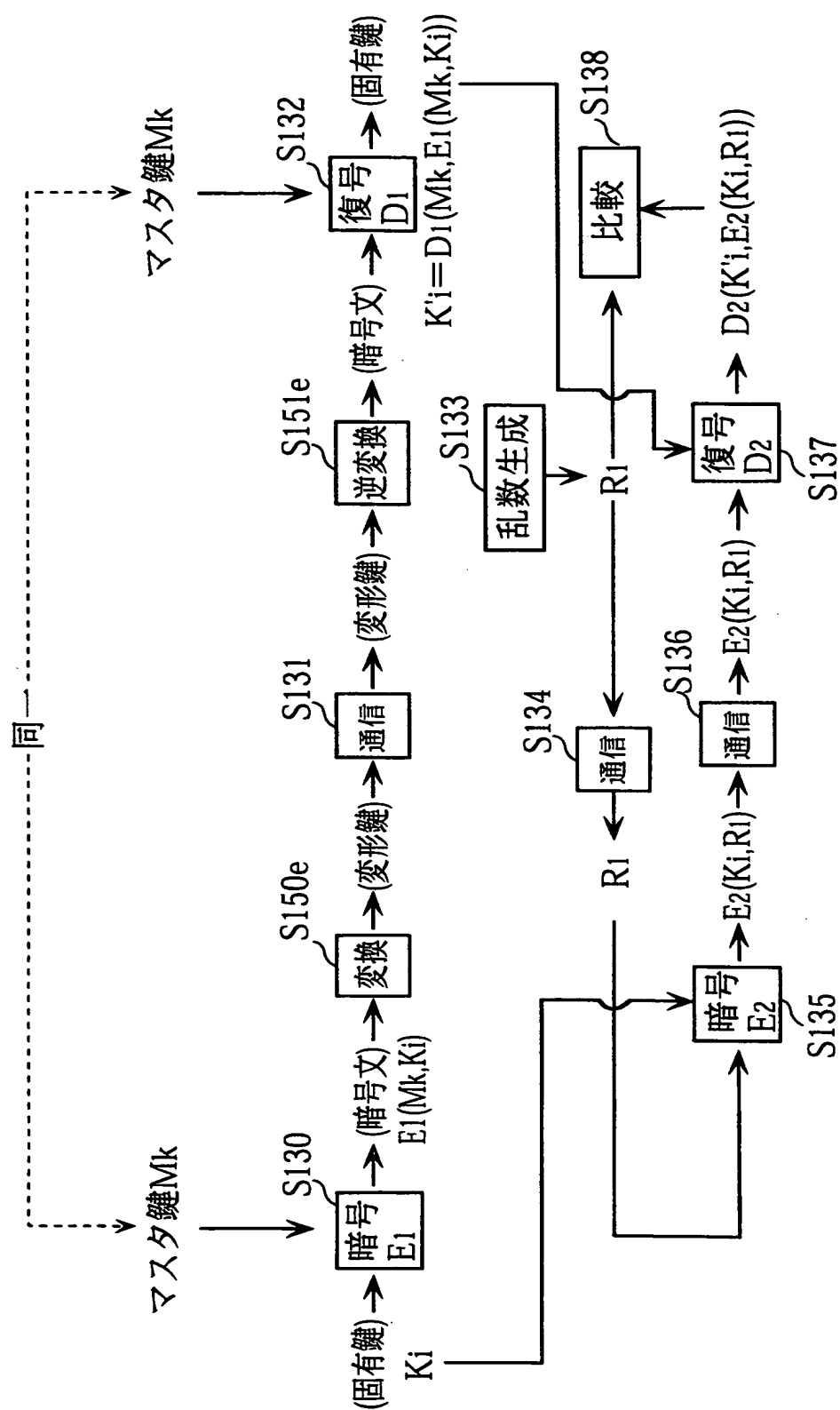
【图 18】



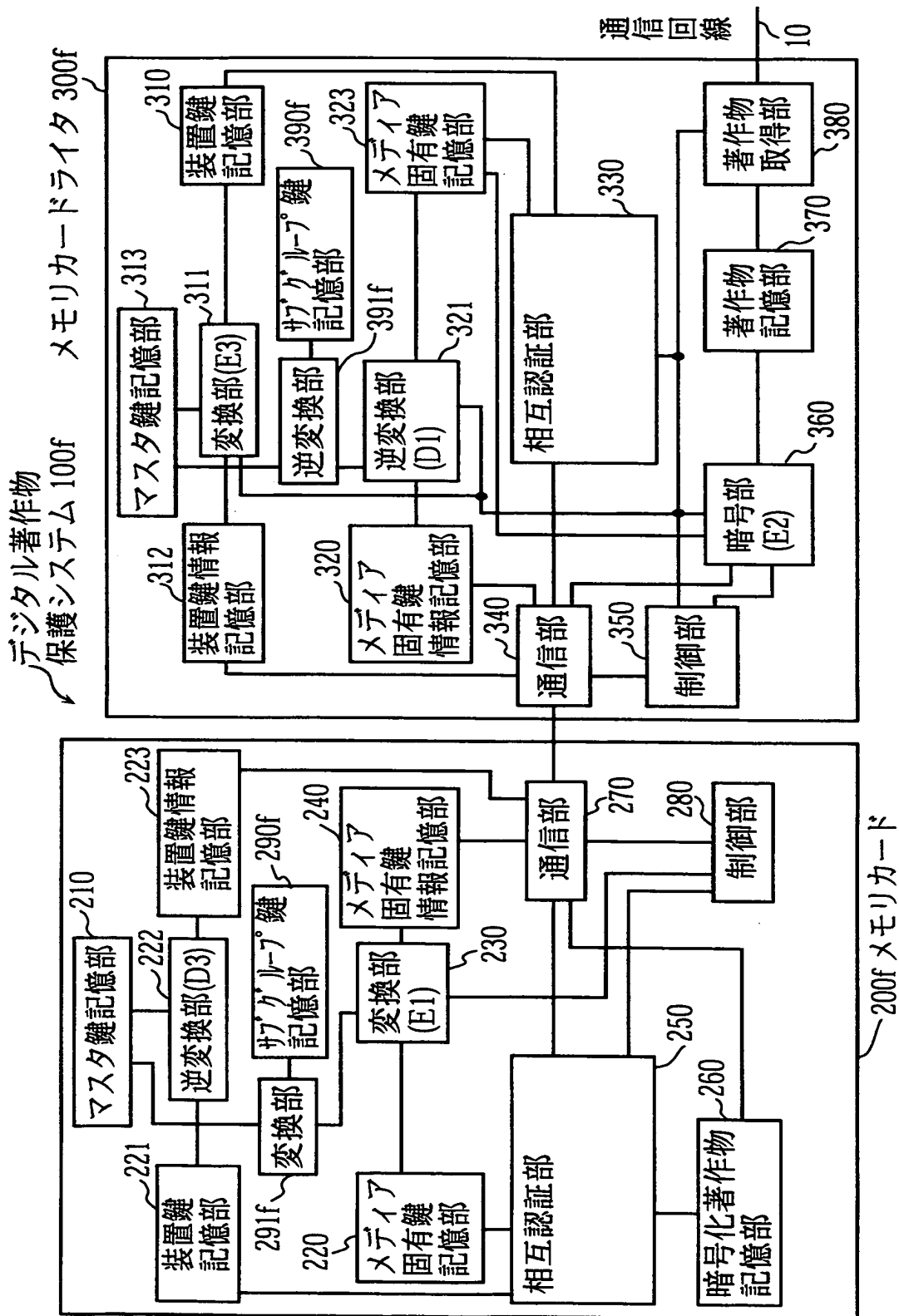
【図 19】



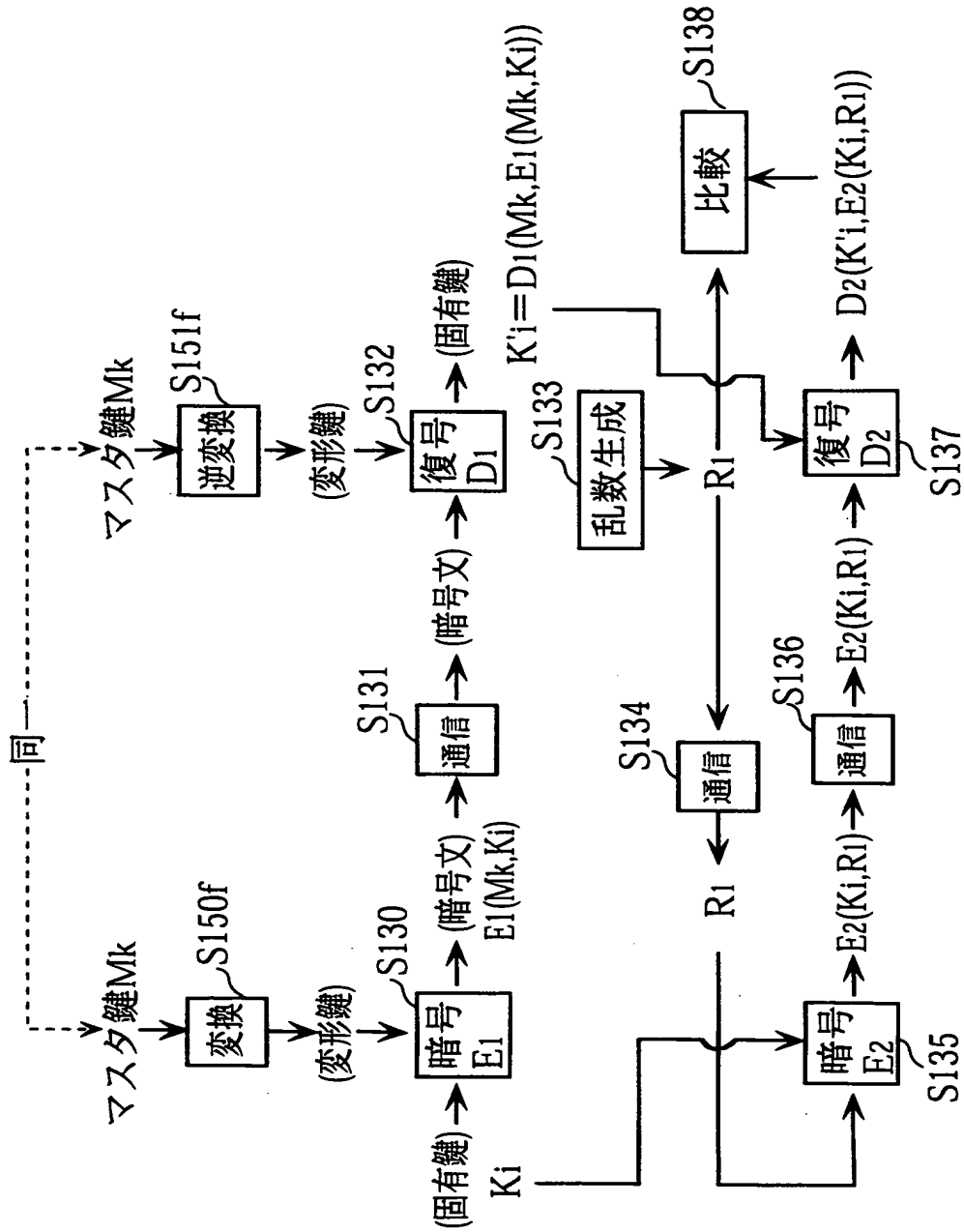
【図 20】



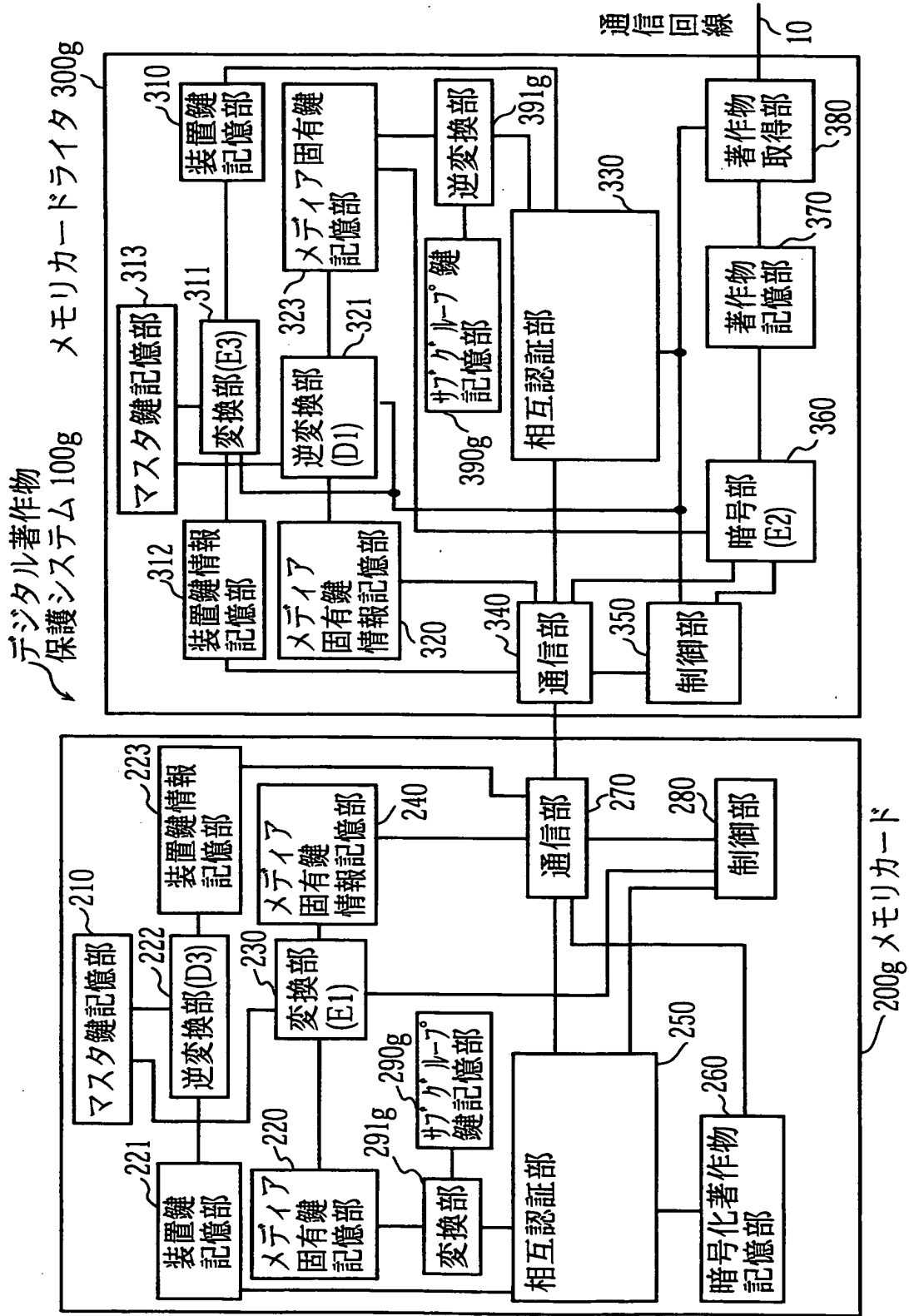
【図 2 1】



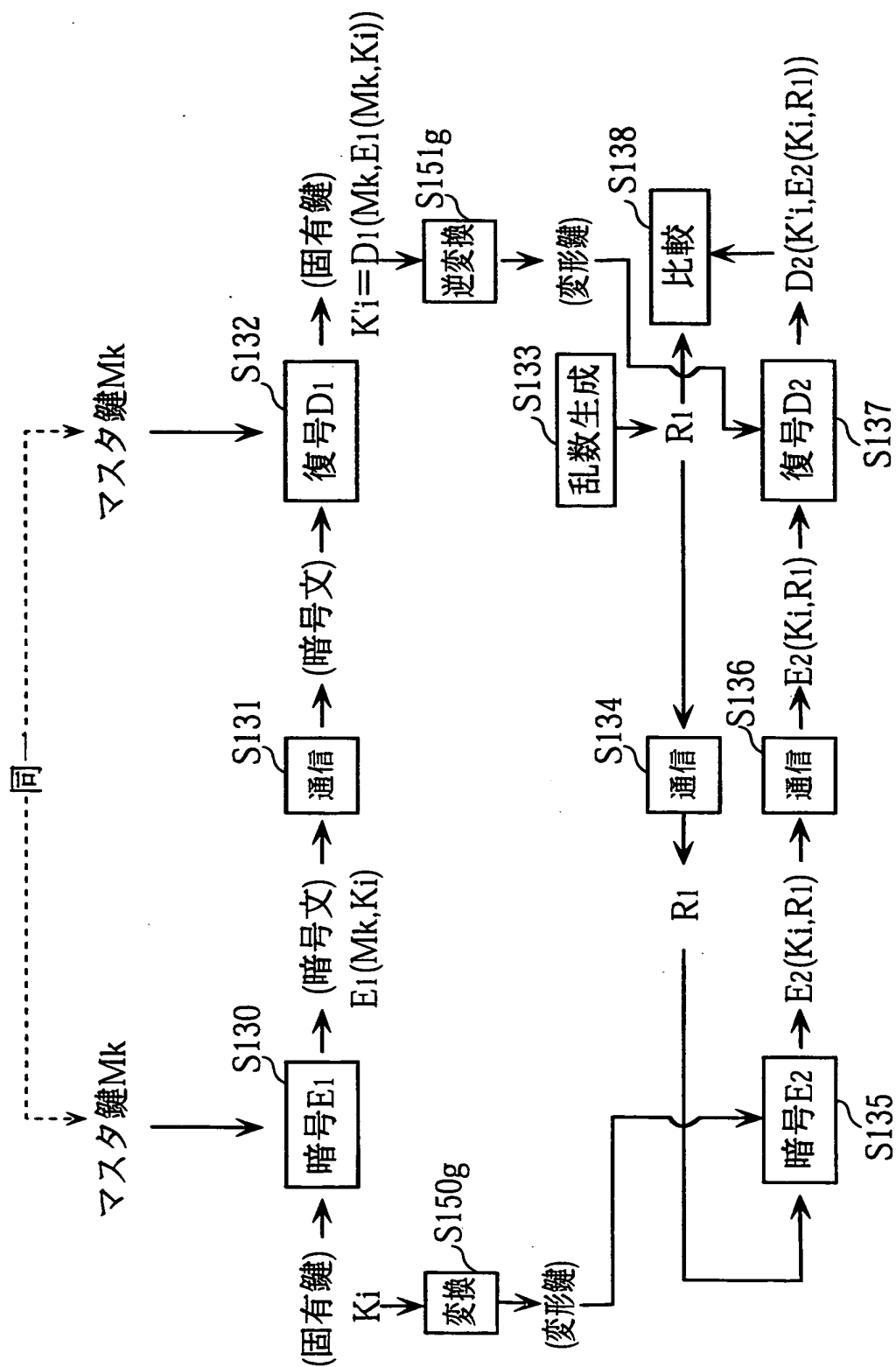
【図 22】



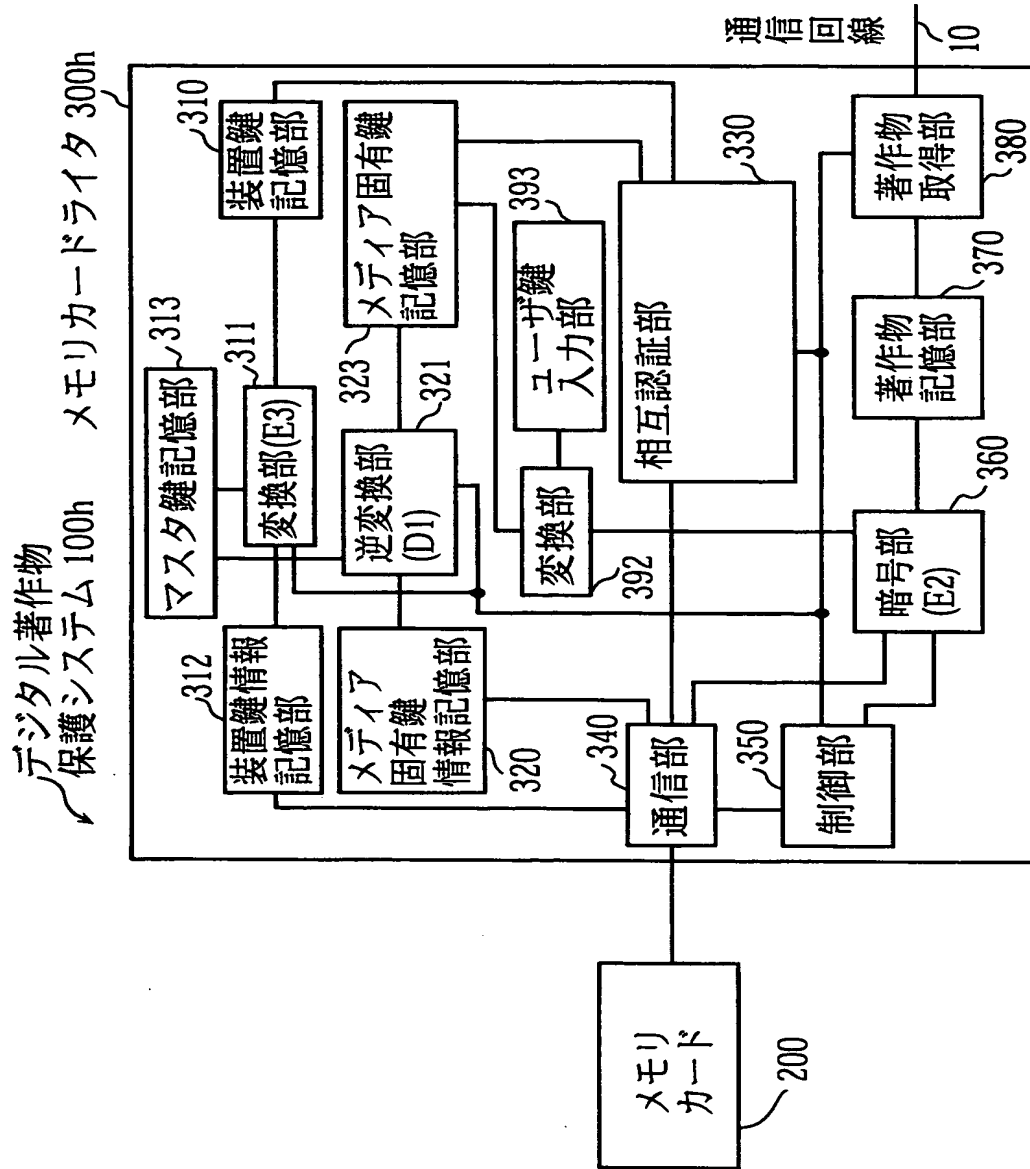
【図 23】



【図 24】

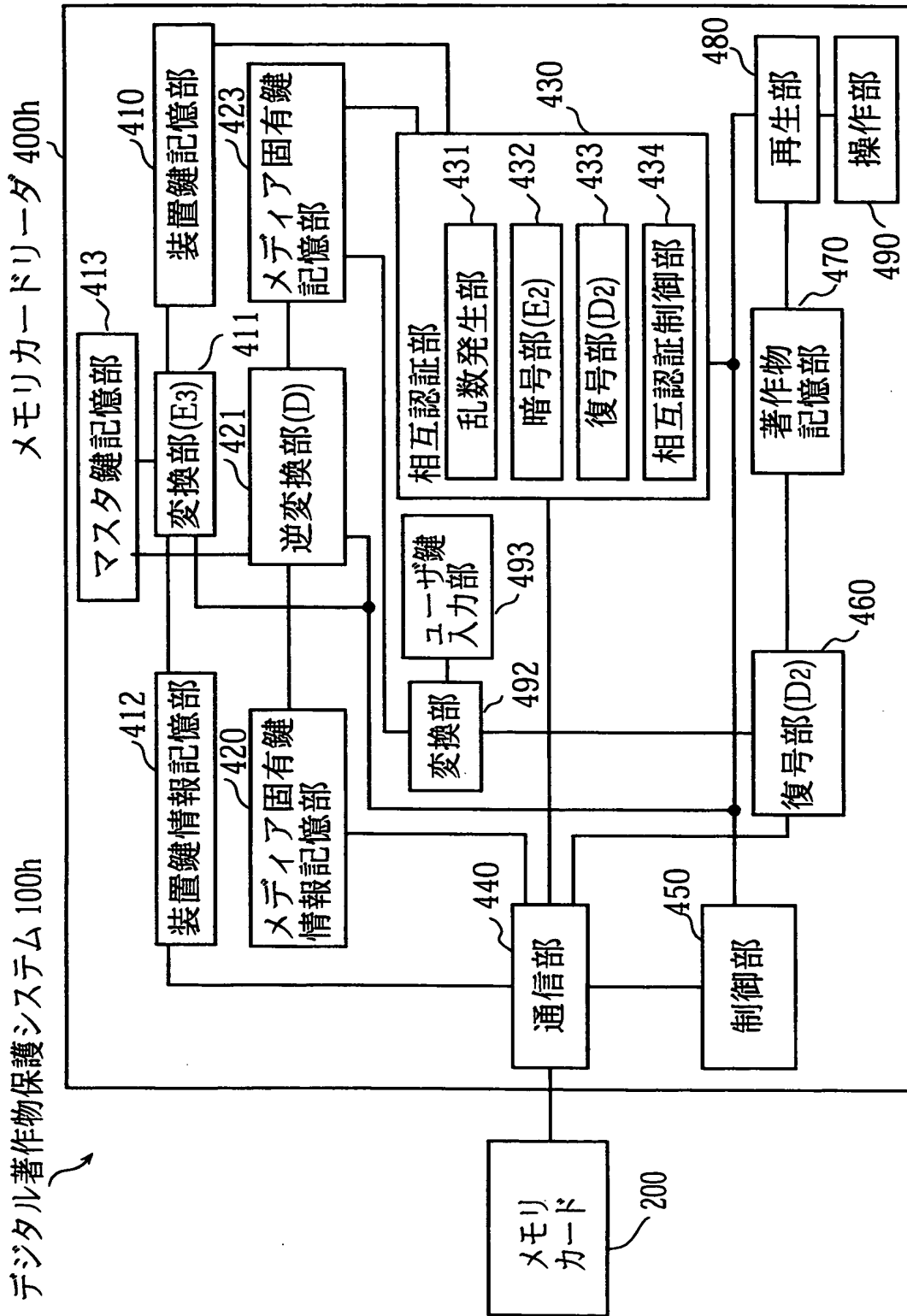


【図 25】

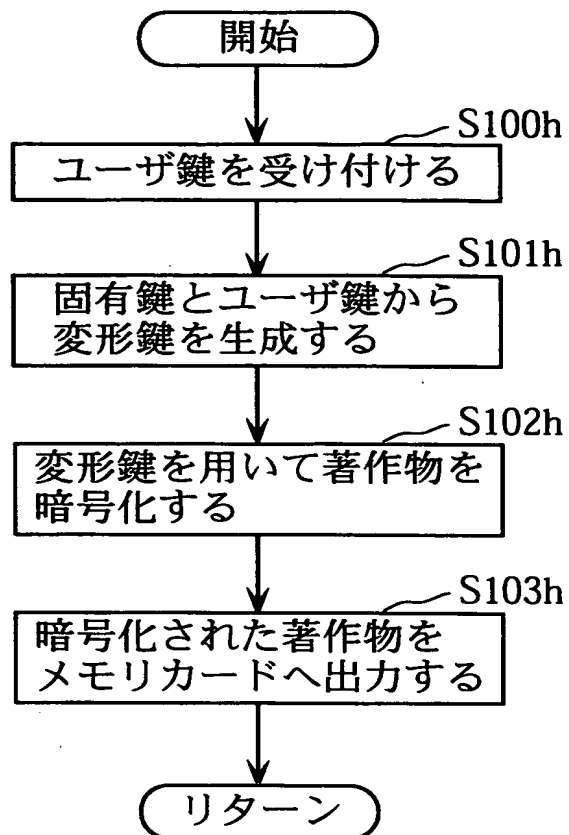




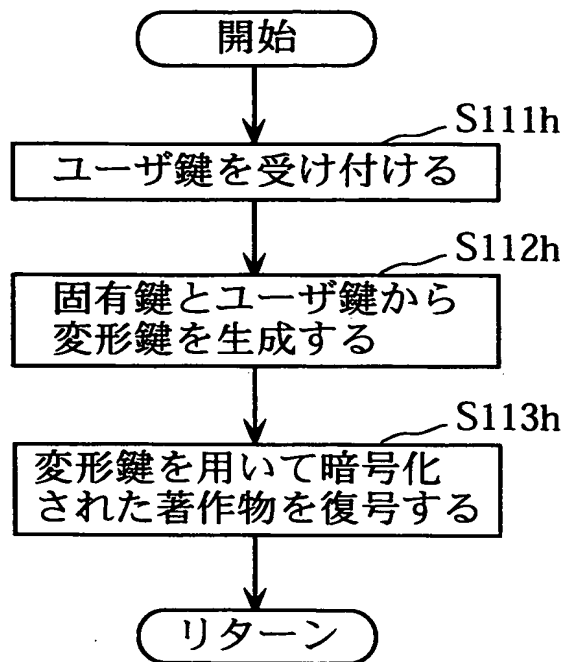
【図 26】



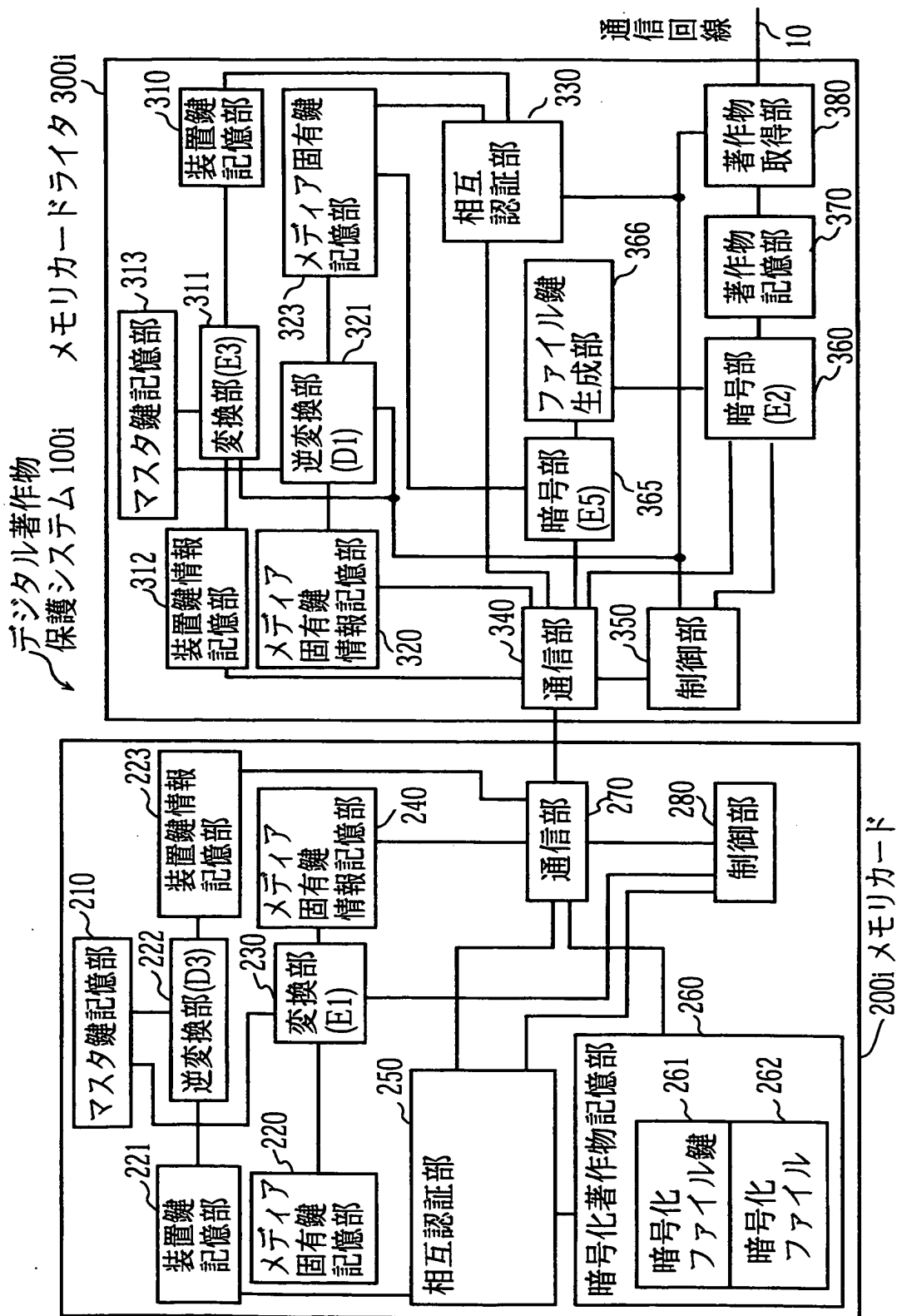
【図 27】



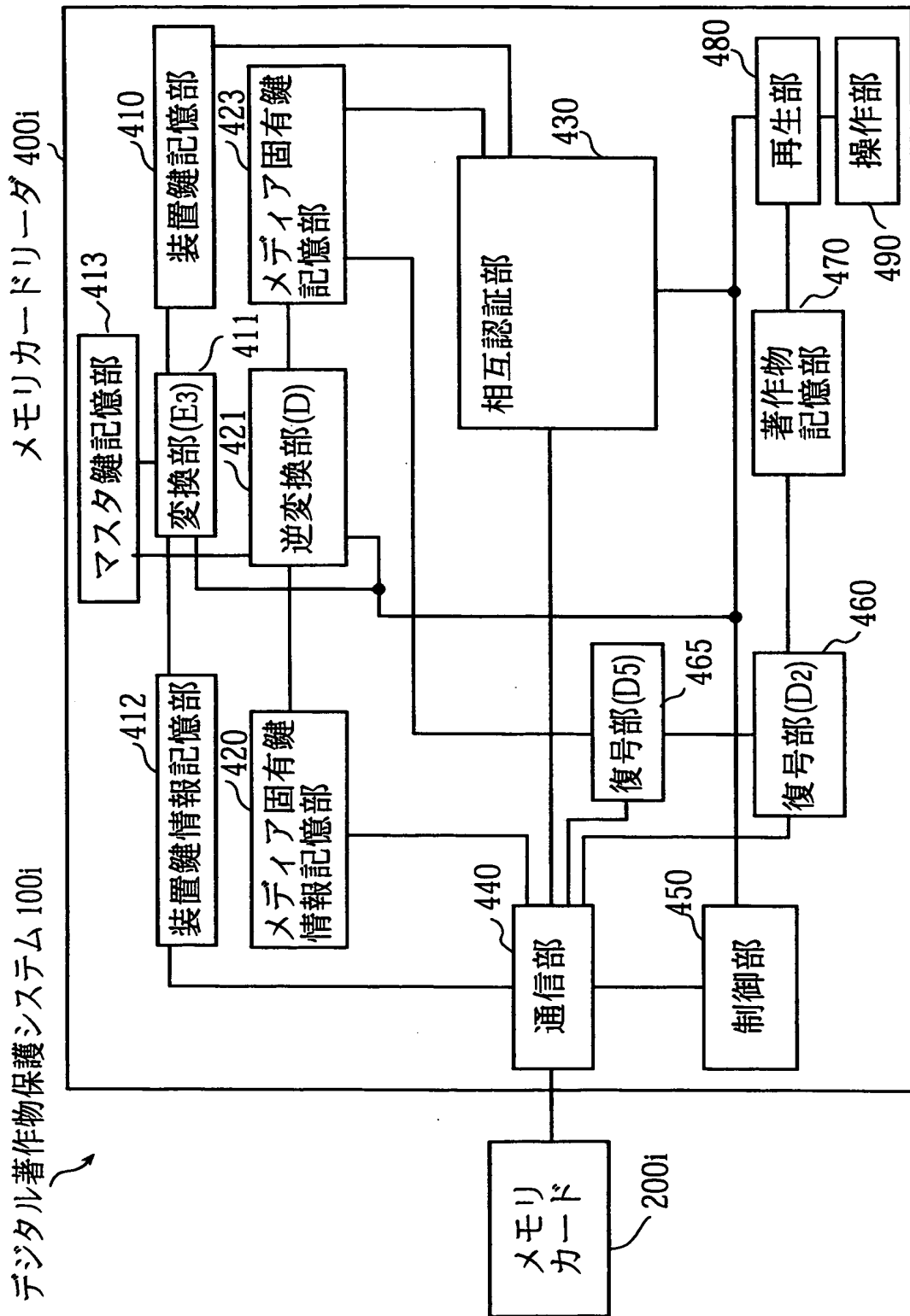
【図 28】



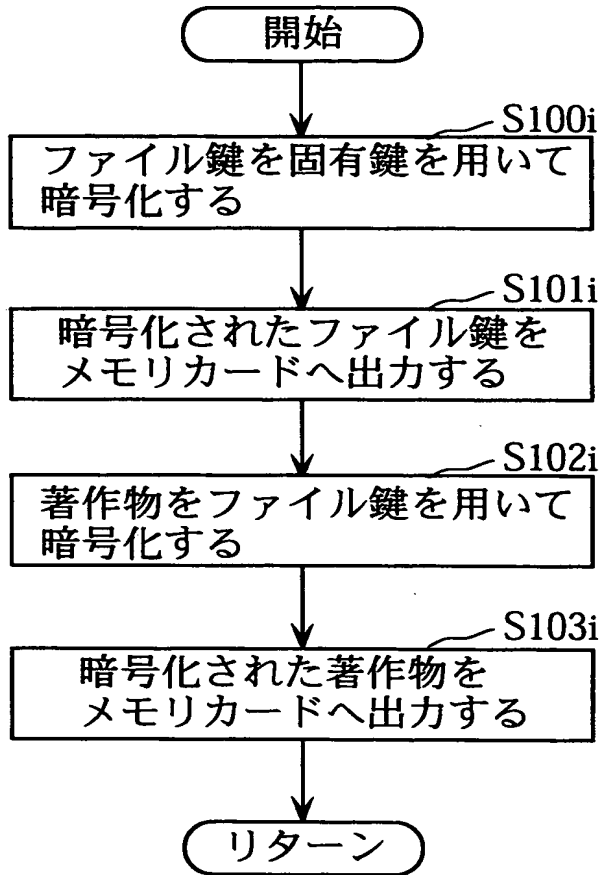
【図 29】



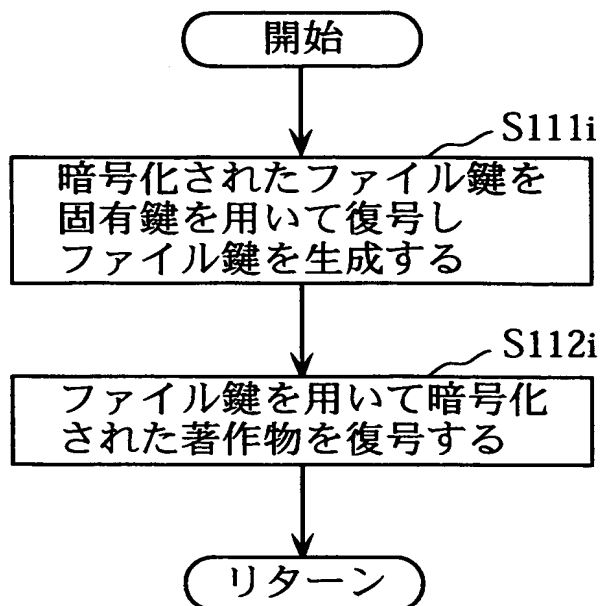
【図 30】



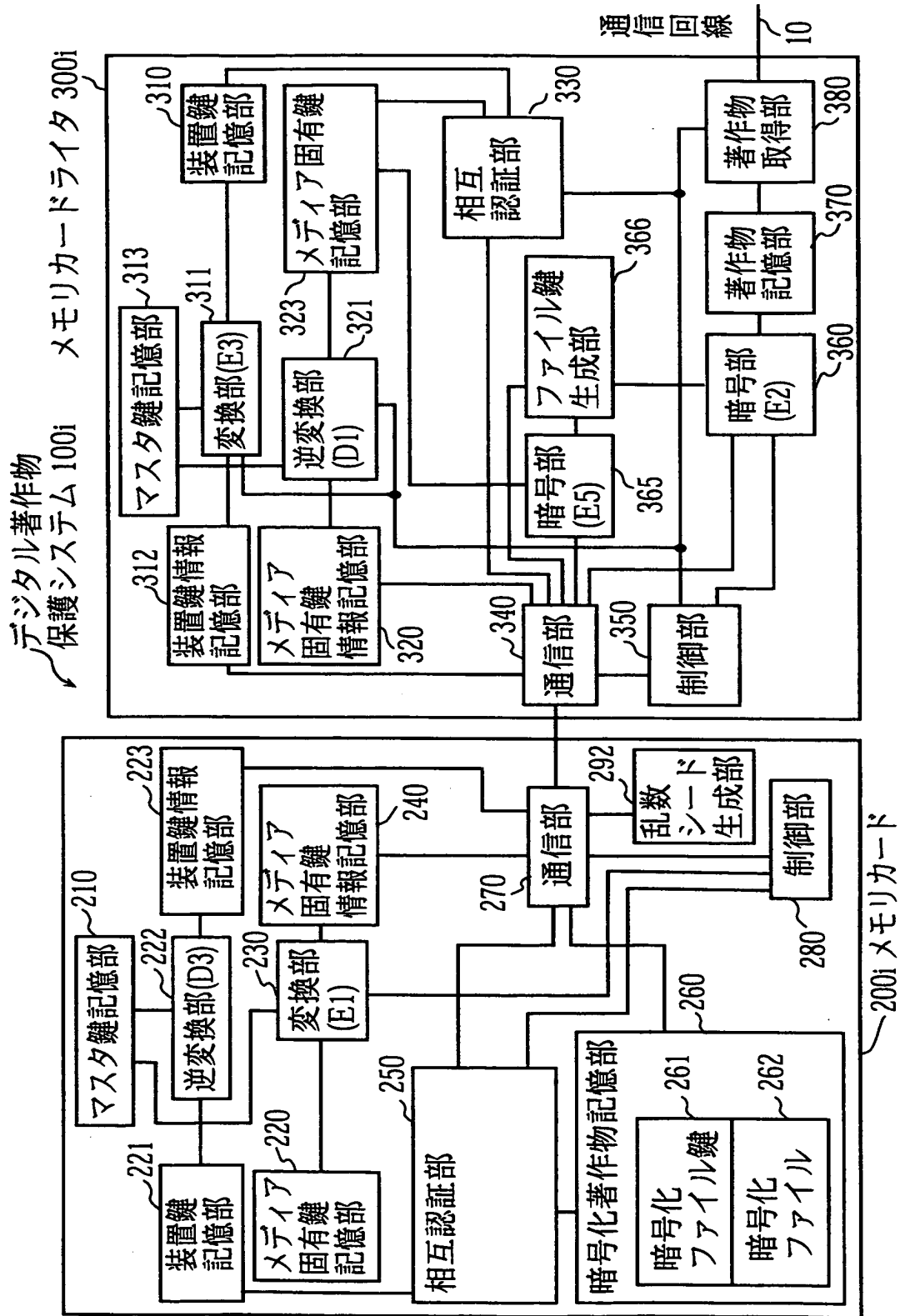
【図 31】



【図 32】

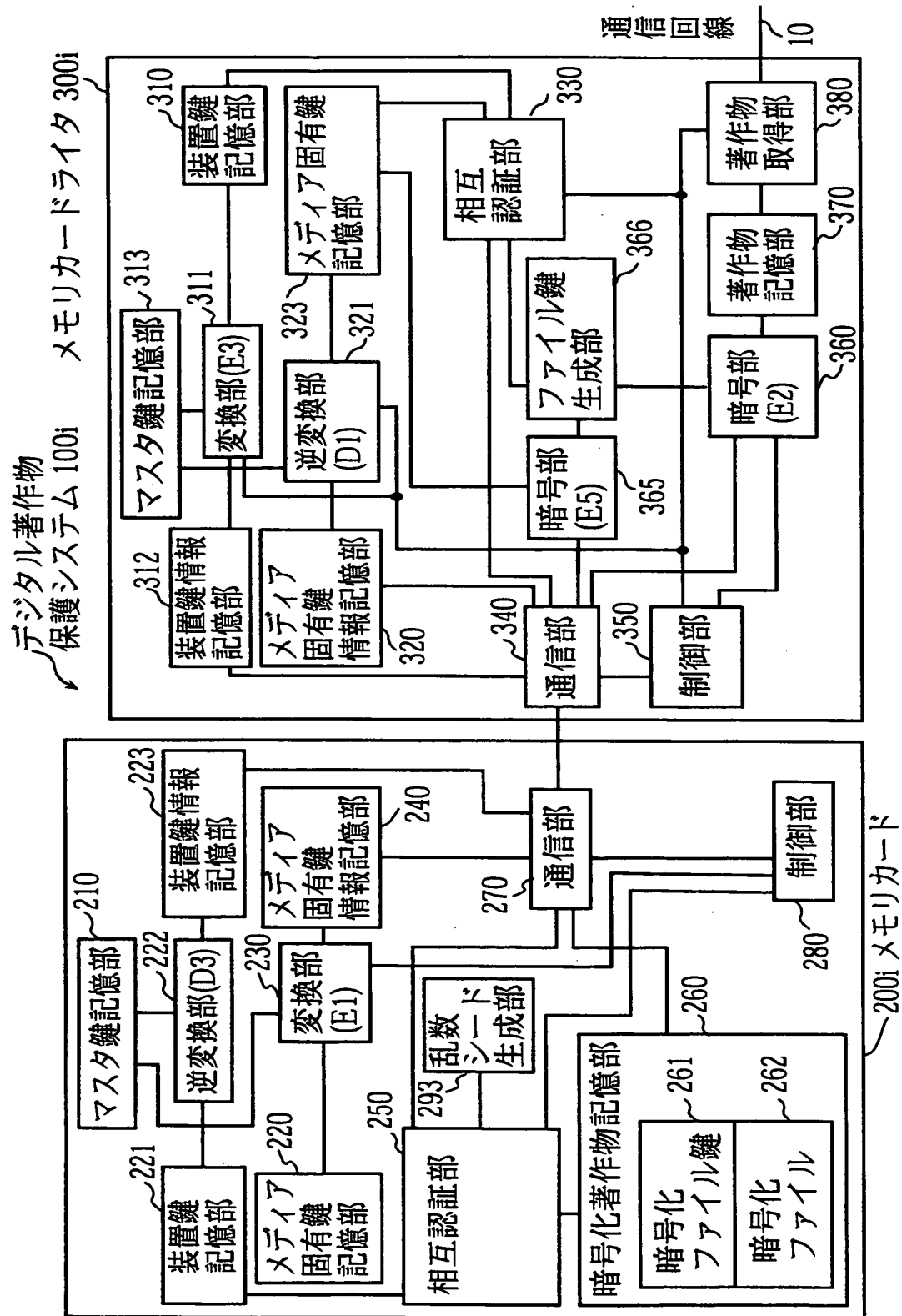


【図 33】





【図 34】



【書類名】 要約書

【要約】

【課題】 外部から取り出したデジタル著作物を不正に記録媒体へ書き込むことと記録媒体に記録されたデジタル著作物を不正に再生することを防止する。

【解決手段】

メディア固有鍵記憶部 220 はあらかじめ一つの固有鍵  $K_i$  を記憶し、変換部 230 は読み出した固有鍵  $K_i$  から暗号化固有鍵  $J_i$  を生成し、乱数発生部 251 は乱数  $R_2$  を生成し、暗号部 252 は乱数  $R_1$  から暗号化乱数  $S_1$  を生成し、復号部 253 は暗号化乱数  $S_2$  から乱数  $R'_2$  を生成し、相互認証制御部 254 は乱数  $R'_2$  と乱数  $R_2$  とを比較し一致すればメモリカード 200 が装着されたメモリカードライタ、メモリカードリーダーが正しい装置と認証する。

【選択図】 図 4

認定・付加情報

特許出願の番号	平成10年 特許願 第339027号
受付番号	59800767744
書類名	特許願
担当官	高田 良彦 2319
作成日	平成11年 4月13日

<認定情報・付加情報>

【特許出願人】

【識別番号】	000005821
【住所又は居所】	大阪府門真市大字門真1006番地
【氏名又は名称】	松下電器産業株式会社

【代理人】

申請人

【識別番号】	100090446
【住所又は居所】	大阪市北区豊崎3丁目2番1号 淀川5番館6F 中島国際特許事務所

【氏名又は名称】	中島 司朗
----------	-------

【代理人】

【識別番号】	100109210
【住所又は居所】	大阪市北区豊崎3丁目2番1号 淀川5番館6F 中島国際特許事務所

【氏名又は名称】	新居 広守
----------	-------

出 願 人 履 歴 情 報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住 所 大阪府門真市大字門真1006番地

氏 名 松下電器産業株式会社